



Red Hat OpenStack Platform 13

릴리스 노트

Red Hat OpenStack Platform 13 릴리스 상세 정보

Red Hat OpenStack Platform 13 릴리스 노트

Red Hat OpenStack Platform 13 릴리스 상세 정보

OpenStack Documentation Team

Red Hat Customer Content Services

rhos-docs@redhat.com

법적 공지

Copyright © 2018 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution-Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

초록

본 문서에서는 Red Hat OpenStack Platform의 주요 기능, 향상된 기능 및 알려진 문제에 대해 간단히 설명합니다.

차례

1장. 소개	3
1.1. 릴리스 정보	3
1.2. 요구 사항	3
1.3. 배포 제한	3
1.4. 데이터베이스 크기 관리	4
1.5. 인증 드라이버 및 플러그인	4
1.6. 인증된 게스트 운영 체제	4
1.7. BARE METAL PROVISIONING에서 지원되는 운영 체제	4
1.8. 하이퍼바이저 지원	4
1.9. CDN(CONTENT DELIVERY NETWORK) 리포지토리	4
1.10. 제품 지원	6
2장. 새로운 주요 기능	7
2.1. RED HAT OPENSTACK PLATFORM DIRECTOR	7
2.2. 컨테이너	7
2.3. BARE METAL 서비스	7
2.4. CEPH STORAGE	7
2.5. COMPUTE	8
2.6. 고가용성	8
2.7. 매트릭스 및 모니터링	8
2.8. 네트워크 기능 가상화	9
2.9. OPENDAYLIGHT	9
2.10. OPENSTACK NETWORKING	10
2.11. 보안	10
2.12. 스토리지	10
2.13. 기술 프리뷰	11
2.13.1. 새로운 기술 프리뷰	11
2.13.2. 이전에 릴리스된 기술 프리뷰	12
3장. 릴리스 정보	14
3.1. RED HAT OPENSTACK PLATFORM 13 GA	14
3.1.1. 기능 개선	14
3.1.2. 기술 프리뷰	16
3.1.3. 릴리스 노트	16
3.1.4. 알려진 문제	19
4장. 기술 노트	27
4.1. RHEA-2018:2086 – RED HAT OPENSTACK PLATFORM 13.0 강화 권고	27

1장. 소개

1.1. 릴리스 정보

본 Red Hat OpenStack Platform 릴리스는 OpenStack "Queens" 릴리스를 기반으로 합니다. 이 릴리스에는 Red Hat OpenStack Platform과 관련된 추가 기능, 알려진 문제, 해결된 문제가 포함되어 있습니다.

Red Hat OpenStack Platform과 관련된 변경 사항만 이 문서에 포함되어 있습니다. OpenStack "Queens"의 자체적 릴리스 노트는 <https://releases.openstack.org/queens/index.html>에서 확인하십시오.

Red Hat OpenStack Platform은 다른 Red Hat 제품의 구성 요소를 사용합니다. 이러한 구성 요소 지원과 관련된 자세한 정보는 다음 링크를 참조하십시오.

<https://access.redhat.com/site/support/policy/updates/openstack/platform/>

Red Hat OpenStack Platform을 평가하려면 다음 링크에서 가입하십시오.

<http://www.redhat.com/openstack/>.



참고

Red Hat Enterprise Linux High Availability Add-On은 Red Hat OpenStack Platform 사용 사례에서 사용할 수 있습니다. 해당 애드온에 대한 자세한 내용은 다음 URL을 참조하십시오: <http://www.redhat.com/products/enterprise-linux-add-ons/high-availability/> Red Hat OpenStack Platform과 함께 사용할 패키지 버전에 대한 자세한 내용은 다음 URL을 참조하십시오: <https://access.redhat.com/site/solutions/509783>

1.2. 요구 사항

Red Hat OpenStack Platform은 Red Hat Enterprise Linux의 최신 릴리스 버전을 지원합니다. 이러한 Red Hat OpenStack Platform 버전은 Red Hat Enterprise Linux 7.5에서 지원됩니다.

Red Hat OpenStack Platform 대시보드는 OpenStack 리소스 및 서비스를 관리할 수 있는 웹 기반 인터페이스입니다. 이번 릴리스의 대시보드는 다음 웹 브라우저의 안정적인 최신 버전을 지원합니다.

- Chrome
- Firefox
- Firefox ESR
- Internet Explorer 11 이상(호환 모드 비활성화)



참고

Red Hat OpenStack Platform을 배포하기 전에 가능한 배포 방식의 특성을 고려해야 합니다. 자세한 내용은 [Installing and Managing Red Hat OpenStack Platform](#) 에서 참조하십시오.

1.3. 배포 제한

Red Hat OpenStack Platform 배포 제한 목록은 [Deployment Limits for Red Hat OpenStack Platform](#) 문서를 참조하십시오.

1.4. 데이터베이스 크기 관리

Red Hat OpenStack Platform 환경에서 MariaDB 데이터베이스의 규모를 유지 관리하는 방법에 대한 권장 사례는 [Database Size Management for Red Hat Enterprise Linux OpenStack Platform](#) 문서를 참조하십시오.

1.5. 인증 드라이버 및 플러그인

Red Hat OpenStack Platform 인증 드라이버 및 플러그인 목록은 [Component, Plug-In, and Driver Support in Red Hat OpenStack Platform](#) 문서를 참조하십시오.

1.6. 인증된 게스트 운영 체제

Red Hat OpenStack Platform 인증된 게스트 운영 체제 목록은 [Certified Guest Operating Systems in Red Hat OpenStack Platform and Red Hat Enterprise Virtualization](#) 문서를 참조하십시오.

1.7. BARE METAL PROVISIONING에서 지원되는 운영 체제

Bare Metal Provisioning (ironic)을 통해 Red Hat OpenStack Platform의 베어 메탈 노드에 설치할 수 있는 지원되는 게스트 운영 체제 목록은 [Supported Operating Systems Deployable With Bare Metal Provisioning \(ironic\)](#)에서 참조하십시오.

1.8. 하이퍼바이저 지원

Red Hat OpenStack Platform은 **libvirt** 드라이버 사용에만 지원됩니다(Compute 노드에서 하이퍼바이저로 KVM 사용).

Ironic은 Red Hat OpenStack Platform 7(Kilo)이 출시된 이후 완전히 지원됩니다. Ironic에서는 일반 기술(예: PXE 부팅 및 IPMI)을 통해 베어 메탈 시스템을 프로비저닝하여 다양한 범주의 하드웨어를 지원하는 동시에 플러그 방식 드라이버를 지원하여 벤더별 기능을 추가할 수 있습니다.

Red Hat은 더 이상 사용되지 않는 VMware "direct-to-ESX" 하이퍼바이저 및 비-KVM libvirt 하이퍼바이저와 같은 기타 Compute 가상화 드라이버를 지원하지 않습니다.

1.9. CDN(CONTENT DELIVERY NETWORK) 리포지토리

이 섹션에서는 Red Hat OpenStack Platform 13 배포에 필요한 리포지토리 설정에 대해 설명합니다.

CDN(Content Delivery Network)을 통해 Red Hat OpenStack Platform 13을 설치할 수 있습니다. 올바른 리포지토리를 사용하도록 **subscription-manager**를 설정합니다.

CDN 리포지토리를 활성화하려면 다음 명령을 실행하십시오.

```
#subscription-manager repos --enable=[reponame]
```

CDN 리포지토리를 비활성화하려면 다음 명령을 실행하십시오.

```
#subscription-manager repos --disable=[reponame]
```

표 1.1. 필수 리포지토리 (x86_64)

리포지토리 이름	리포지토리 레이블
Red Hat Enterprise Linux 7 Server (RPMS)	rhel-7-server-rpms
Red Hat Enterprise Linux 7 Server - RH Common (RPMS)	rhel-7-server-rh-common-rpms
Red Hat Enterprise Linux High Availability (for RHEL 7 Server)	rhel-ha-for-rhel-7-server-rpms
Red Hat OpenStack Platform 13 for RHEL 7(RPMS)	rhel-7-server-openstack-13-rpms
Red Hat Enterprise Linux 7 Server - Extras(RPMS)	rhel-7-server-extras-rpms

표 1.2. 선택적 리포지토리 (x86_64)

리포지토리 이름	리포지토리 레이블
Red Hat Enterprise Linux 7 Server - Optional	rhel-7-server-optional-rpms
Red Hat OpenStack Platform 13 Operational Tools for RHEL 7(RPMS)	rhel-7-server-openstack-13-optools-rpms

표 1.3. 필수 리포지토리 (ppc64le)

리포지토리 이름	리포지토리 레이블
Red Hat Enterprise Linux for IBM Power, little endian	rhel-7-for-power-le-rpms
Red Hat OpenStack Platform 13 for RHEL 7(RPMS)	rhel-7-server-openstack-13-for-power-le-rpms

비활성화할 리포지토리

다음 표에서는 Red Hat OpenStack Platform 13이 올바르게 작동하기 위해 비활성화해야 하는 리포지토리에 대해 간단히 설명합니다.

표 1.4. 비활성화할 리포지토리

리포지토리 이름	리포지토리 레이블
Red Hat CloudForms Management Engine	"cf-me-"
Red Hat Enterprise Virtualization	"rhel-7-server-rhev"
Red Hat Enterprise Linux 7 Server - Extended Update Support	"*-eus-rpms"



주의

Red Hat OpenStack Platform 소프트웨어 리포지토리의 일부 패키지는 EPEL(Extra Packages for Enterprise Linux) 소프트웨어 리포지토리에서 제공하는 패키지와 충돌하는 경우가 있습니다. EPEL 소프트웨어 리포지토리가 활성화된 시스템에서 Red Hat OpenStack Platform을 사용하는 것은 지원되지 않습니다.

1.10. 제품 지원

다음 리소스를 사용할 수 있습니다:

고객 포털

Red Hat 고객 포털은 OpenStack 배포 계획, 배포 및 유지 보수를 지원하기 위해 다양한 리소스를 제공합니다. 고객 포털을 통해 이용할 수 있는 기능은 다음과 같습니다.

- 지식 베이스 문서 및 솔루션
- 기술 요약
- 제품 설명서
- 기술 지원 사례 관리

<https://access.redhat.com/>에서 고객 포털에 액세스하십시오.

메일링 리스트

Red Hat은 OpenStack 사용자와 관련된 공개 메일링 리스트를 제공합니다.

- **rhsa-announce** 메일링 리스트는 Red Hat OpenStack Platform을 포함하여 모든 Red Hat 제품의 보안 수정 릴리스에 대한 알림을 제공합니다.

<https://www.redhat.com/mailman/listinfo/rhsa-announce>에서 가입하십시오.

2장. 새로운 주요 기능

이 섹션에서는 이번 Red Hat OpenStack Platform 릴리스의 새로운 주요 기능에 대해 설명합니다.

2.1. RED HAT OPENSTACK PLATFORM DIRECTOR

이 섹션에서는 director의 새로운 주요 기능에 대해 간단히 설명합니다.

빠른 업그레이드

Director는 특히 Red Hat OpenStack Platform 10에서 Red Hat OpenStack Platform 13까지 여러 버전을 통해 빠른 업그레이드 경로를 제공합니다. 이 기능은 사용자가 긴 수명 버전으로 되어 있는 특정 OpenStack 버전을 계속 사용하다가 다음의 긴 수명 버전이 제공될 때 업그레이드할 수 있도록 하기 위한 것입니다. 전체 지침은 [Fast Forward Upgrades 가이드](#)에서 확인할 수 있습니다.

L3 라우팅 스파인-리프형 네트워크

Director는 프로비저닝 및 인트로스펙션 기능을 위해 여러 네트워크를 정의할 수 있습니다. 구성 가능한 네트워크와 함께 이 기능을 사용하면 사용자가 오버클라우드에 대해 완전히 L3 라우팅된 스파인-리프(spine-leaf)형 아키텍처를 프로비저닝하고 설정할 수 있습니다. 전체 지침은 [Spine Leaf Networking 가이드](#)에서 확인할 수 있습니다.

Red Hat Virtualization 드라이버

Director OpenStack Bare Metal(ironic) 서비스는 Red Hat Virtualization 환경 내에서 가상 노드를 관리하는 드라이버가 포함되어 있습니다. 이를 통해 director는 Red Hat Virtualization에 배포된 컨트롤러 노드를 사용하여 오버클라우드를 프로비저닝하고 지원할 수 있습니다. 새 가상화 기능에 대한 자세한 내용은 [Virtualize your OpenStack control plane with Red Hat Virtualization and Red Hat OpenStack Platform 13](#)에서 참조하십시오.

2.2. 컨테이너

이 섹션에서는 Red Hat OpenStack Platform에서 컨테이너화를 위한 새로운 주요 기능에 대해 간단히 설명합니다.

완전히 컨테이너화된 서비스

이번 릴리스에서는 이전 버전에서 컨테이너화되지 않았던 OpenStack Networking(neutron), OpenStack Block Storage(cinder) 및 OpenStack Shared File Systems(manila) 서비스를 포함하여 모든 Red Hat OpenStack Platform 서비스를 컨테이너로 제공합니다. 오버클라우드에는 이제 완전히 컨테이너화된 서비스를 사용합니다.

2.3. BARE METAL 서비스

이 섹션에서는 Bare Metal(ironic) 서비스의 새로운 주요 기능에 대해 간단히 설명합니다.

2.4. CEPH STORAGE

이 섹션에서는 Ceph Storage의 새로운 주요 기능에 대해 간단히 설명합니다.

Red Hat Ceph Storage 3.0 지원

이번 릴리스에서 Red Hat Ceph Storage 3.0(luminous)은 Red Hat OpenStack에서 지원하는 Ceph의 기본 버전이며 director의 기본 배포 버전입니다. Ceph는 이제 버전 2.x에서 3까지 롤링 업그레이드를 지원합니다. director를 사용하여 Ceph 클러스터를 배포하는 경우 새 OpenStack 릴리스로 업그레이드하면 Red Hat Ceph Storage도 3.0으로 업그레이드됩니다.

Ceph 메타데이터 서버 및 RADOS 게이트웨이 노드 확장

Red Hat Ceph Storage 3.0은 CephFS(Ceph 파일 시스템)의 적절하게 설정하여 MDS(다중 메타데이터

서버)에서 메타데이터 로드 확장을 추가 지원합니다. 설정이 완료되면 **Ceph** 클러스터에서 사용할 수 있는 추가 전용 **MDS** 서버가 이 추가 로드를 사용할 수 있도록 자동으로 할당됩니다. 또한 새로운 전용 **Ceph RGW(RADOS 게이트웨이)** 노드를 추가하여 **RGW**를 필요에 따라 확장할 수 있습니다.

NFS를 사용하는 Manila CephFS 스토리지

Shared File System 서비스(**manila**)는 **NFSv4** 프로토콜을 통해 **CephFS**(**Ceph** 파일 서비스)에서 지원하는 공유 파일 시스템 마운트를 지원합니다. 컨트롤러 노드에서 운영되는 **NFS-Ganesha** 서버는 **CephFS**를 **HA**(고가용성)의 테넌트로 내보내는 데 사용됩니다. 테넌트는 서로 격리되며 제공된 **NFS** 게이트웨이 인터페이스를 통해서만 **CephFS**에 액세스할 수 있습니다. 이 새로운 기능은 **director**에 모두 통합되어 **CephFS** 백엔드 배포 및 **Shared File System** 서비스의 설정을 가능하게 합니다.

다중 Cinder Ceph 풀 지원 강화

Block Storage(cinder) **RBD(RADOS 블록 장치)** 백엔드는 **director** 템플릿 매개 변수 **CinderRbdExtraPools**를 사용하여 동일한 **Ceph** 클러스터 내에서 다른 풀에 매핑할 수 있습니다. 새로운 **Block Storage RBD** 백엔드는 **CinderRbdPoolName** 매개 변수와 연결된 표준 **RBD** 백엔드 외에도 이 매개 변수와 연결된 각 **Ceph** 풀에 대해 생성됩니다.

ceph-ansible을 사용하는 RBD 미러 director

Ceph rbd-mirror 데몬은 원격 클러스터에서 이미지 업데이트를 가져와서 로컬 클러스터 내에서 이미지에 업데이트를 적용합니다. **RBD** 미러는 **Red Hat Ceph Storage 3.0(luminous)**과 함께 **ceph-ansible**을 사용하여 컨테이너로 배포됩니다. 해당 이미지와 관련된 **OpenStack** 메타데이터는 **rbd-mirror**로 복사되지 않습니다.

2.5. COMPUTE

이 섹션에서는 **Compute** 서비스의 새로운 주요 기능에 대해 간단히 설명합니다.

실시간 KVM 통합

Compute 서비스와의 실시간 **KVM(RT-KVM)** 통합은 이제 완전히 지원됩니다. **RT-KVM**의 이점은 다음과 같습니다.

- 시스템 호출 및 인터럽트에 대해 명확하게 낮은 평균대기 시간
- 정확한 시간 동기화를 위해 게스트 인스턴스에 **PTP(Precision Time Protocol)** 지원(이 릴리스에 대한 커뮤니티 지원)

2.6. 고가용성

이 섹션에서는 고가용성의 새로운 주요 기능에 대해 간단히 설명합니다.

인스턴스 HA에 대한 Director 통합

이제 **director**를 사용하여 인스턴스 **HA**를 배포할 수 있습니다. 따라서 추가적인 수동 구성없이 인스턴스 **HA**를 설치 및 업그레이드할 수 있습니다.



참고

인스턴스 **HA**의 **Director** 통합 기능은 버전 **13** 이상에서만 사용할 수 있습니다. 빠른 업그레이드를 포함하여 이전 버전에서 버전 **13**으로 업그레이드하려면 먼저 인스턴스 **HA**를 수동으로 비활성화해야 합니다.

2.7. 매트릭스 및 모니터링

이 섹션에서는 매트릭스 및 모니터링 구성 요소에 대한 새로운 주요 기능 및 변경사항에 대해 간단히 설명합니다.

collectd 5.8 통합

collectd 5.8 버전에는 다음의 추가 플러그인이 포함됩니다.

- **ovs-stats** - 플러그인은 OVS가 연결된 브릿지 및 인터페이스의 통계를 수집합니다.
- **ovs-events** - 플러그인은 OVS(Open vSwitch)가 연결된 인터페이스의 연결 상태를 모니터링하고 값을 collectd에 보내어 OVS 데이터베이스에서 연결 상태가 변경될 때마다 알림을 보냅니다.
- **hugepages - hugepages** 플러그인을 통해 플랫폼에서 사용 가능한 hugepage를 개수, 바이트, 또는 백분율로 모니터링합니다.
- **intel-rdt - intel_rdt** 플러그인은 CMT(Cache Monitoring Technology), MBM(Memory Bandwidth Monitoring) 같은 Intel® RDT(Intel Resource Director Technology)의 기능을 모니터링하여 제공되는 정보를 수집합니다. 이러한 기능은 LLC(Last level cache, 최종 레벨 캐시) 점유율, 로컬 메모리 대역폭 사용, 원격 메모리 대역폭 사용 및 IPC(Instructions per Clock, 클럭 당 명령어 처리 수) 등의 공유 리소스 사용에 관한 정보를 제공합니다.
- **libvirt** 플러그인 확장 - **libvirt** 플러그인이 확장되어 플랫폼에서 CMT, MBM, CPU 고정, 사용률 및 상태 매트릭스를 지원하게 되었습니다.

collectd 및 gnocchi 통합

collectd-gnocchi 플러그인은 매트릭스를 gnocchi에 전송합니다. 기본적으로 **collectd**라는 리소스 유형 및 모니터링되는 각 호스트에 대한 새 리소스를 생성합니다. 각 호스트에는 다음의 이름 지정 규칙을 통해 동적으로 생성된 매트릭스 목록이 있습니다.

```
plugin-plugin_instance/type-type_instance-value_number
```

매트릭스를 적절하게 생성하려면 보관 정책 규칙이 일치하는지 확인하십시오.

다중 RabbitMQ 서버를 사용하여 sensu 지원

이번 릴리스를 통해 Red Hat OpenStack Platform은 다중 RabbitMQ 서버를 사용하여 **sensu**를 추가 지원합니다. 이를 위해 **config.yaml** 파일에서 **MonitoringRabbitCluster** 매개 변수를 사용해야 합니다.

Intel Resource Director Technology/Memory Bandwidth Monitoring 지원

MBM(Memory Bandwidth Monitoring)은 Intel® RDT(Resource Director Technology)의 필수 요소입니다. 메모리 사용률 및 가용성 정보는 모든 노드에서 수집되며 이러한 정보에 기반하여 OpenStack에서 더 나은 스케줄링 결정을 내리고 SLA에 이를 전달하도록 사용할 수 있습니다.

2.8. 네트워크 기능 가상화

이 섹션에서는 NFV(Network Functions Virtualization)의 새로운 주요 기능에 대해 간단히 설명합니다.

NFV 워크로드에 대한 실시간 KVM Compute 역할

실시간 KVM(RT-KVM) Compute 노드에는 이제 RT-KVM Compute 노드 역할이 추가되어 NFV 워크로드를 지원합니다. 이 새로운 역할은 실시간 기능을 통해 Compute 노드의 일부를 공개하고 엄격한 대기 시간 요구 사항이 있는 게스트를 지원합니다.

2.9. OPENDAYLIGHT

이 섹션에서는 OpenDaylight 서비스의 새로운 주요 기능에 대해 간단히 설명합니다.

OpenDaylight 통합

OpenDaylight는 유연한 모듈식 개방형 SDN 플랫폼으로, Red Hat OpenStack Platform 릴리스에서 완전히 지원됩니다. 현재 Red Hat 지원 제품은 OpenDaylight SDN 컨트롤러를 OpenStack의 네트워킹 백엔드로 활성화하도록 설계되어 엄선된 OpenDaylight 구성 요소를 결합합니다. 이 솔루션에서 사용되는 주요 OpenDaylight 프로젝트는 OpenStack neutron API에 대한 지원이 포함된 NetVirt입니다. 자세한 내용은 [Red Hat OpenDaylight Product Guide](#) 및 [Red Hat OpenDaylight Installation and Configuration Guide](#)에서 참조하십시오.

2.10. OPENSTACK NETWORKING

이 섹션은 Networking 서비스의 새로운 주요 기능에 대해 간단히 설명합니다.

Octavia LBaaS

Octavia는 이제 완전히 지원됩니다. Octavia는 로드 밸런싱 기능을 제공하는 공식 OpenStack 프로젝트로 기존 HAProxy 기반 구현을 대체하도록 고안되었습니다. Octavia는 LBaaS v2 API를 구현하지만 추가적인 기능도 제공합니다. Octavia에는 *amphora*(Compute VM으로 구현됨)와의 로드 밸런싱을 제공하는 레퍼런스 로드 밸런싱 드라이버가 포함되어 있습니다.

OVN(Open Virtual Network)

OVN은 이제 완전히 지원됩니다. OVN은 네트워크 서비스를 인스턴스에 제공하는 Open vSwitch 기반 네트워크 가상화 솔루션입니다. OVN은 **neutron API**를 완전 지원합니다.

2.11. 보안

이 섹션에서는 보안 구성 요소의 새로운 주요 기능에 대해 간단히 설명합니다.

Barbican

OpenStack Key Manager(**barbican**)는 Red Hat OpenStack Platform의 암호 관리자입니다. Barbican API 및 명령줄로 OpenStack 서비스에서 사용하는 인증서, 키 및 암호를 중앙에서 관리할 수 있습니다.

Barbican - 암호화된 볼륨 지원

Barbican을 사용하여 Block Storage (**cinder**) 암호화 키를 관리할 수 있습니다. 이 설정에서는 LUKS를 사용하여 부팅 디스크 등 인스턴스와 연결된 디스크를 암호화합니다. 키 관리는 사용자가 알 수 있도록 투명하게 수행됩니다.

Barbican - glance 이미지 서명

Image Service(**glance**)를 설정하여 업로드된 이미지가 변경되지 않았는지를 확인할 수 있습니다. 이미지는 먼저 **barbican**에 저장된 키로 서명된 다음 매번 이미지를 사용하기 전에 확인됩니다.

PDP(Policy Decision Points)와의 통합

리소스에 대한 액세스를 제어하는 데 PDP(Policy Decision Points)를 사용하는 고객의 경우 Identity 서비스(**keystone**)에서 인증 확인을 위해 외부 PDP와 프로젝트를 통합할 수 있습니다. 외부 PDP는 액세스 요청을 평가하고 설정된 정책에 따라 액세스를 부여하거나 거부할 수 있습니다.

인프라 및 가상화 기능 강화

AIDE 침입 감지 기능은 이제 기술 프리뷰로 사용할 수 있습니다. Director의 AIDE 서비스를 통해 운영자는 침입 감지 규칙 세트를 중앙에서 설정한 다음 오버클라우드에서 AIDE를 설치하고 설정할 수 있습니다.

2.12. 스토리지

이 섹션에서는 스토리지 구성 요소의 새로운 주요 기능에 대해 간단히 설명합니다.

Block Storage - Block Storage 서비스의 컨테이너화된 배포

이번 릴리스에서 **Block Storage** 서비스(cinder)의 컨테이너화된 배포는 기본 기능입니다. **Block Storage** 서비스에 대해 외부 설치 종속성을 지닌 백엔드를 사용하는 경우 배포에 대한 벤더별 컨테이너를 가져와야 합니다.

Block Storage - 다중 백엔드 가용성 영역

Block Storage 서비스(cinder)를 통해 이제 설정 파일의 백엔드 섹션에서 새 드라이버 설정 옵션인 **backend_availability_zone**을 사용하여 백엔드 가용성 영역을 정의할 수 있습니다. 이전 버전에서는 **cinder-volume**에 설정된 백엔드가 동일한 스토리지 가용성 영역의 일부여야 했습니다.

Block Storage - OpenStack Key Manager 지원

Block Storage 서비스(cinder)는 이제 **OpenStack Key Manager**(barbican)를 사용하여 볼륨 암호화에 사용되는 암호화 키를 저장할 수 있습니다. 이 기능은 **director**에서 **OpenStack Key Manager**를 설정하면 활성화됩니다. 새로운 키는 **Identity** 서비스(keystone)의 **admin** 또는 **creator** 역할로 사용자가 **OpenStack Key Manager**에 추가할 수 있습니다.

Block Storage - RBD 드라이버 암호화 지원

RBD 드라이버는 이제 **LUKS**를 사용하여 **Block Storage** 서비스(cinder) 볼륨 암호화를 처리합니다. 이 기능은 미사용 데이터 보안을 제공하도록 **Block Storage** 서비스와 **Compute** 서비스를 사용하여 **RBD**에서 볼륨을 암호화하는 기능을 제공합니다. **OpenStack Key Manager**(barbican)는 **RBD** 드라이버 암호화를 사용하는 데 필요합니다. **RBD** 드라이버 암호화는 **Block Storage** 서비스에서만 지원됩니다.

Image 서비스 - 이미지 서명 및 검증 지원

Image 서비스(glance)는 이제 **OpenStack Key Manager**(barbican)를 사용하여 부팅 가능한 이미지의 서명 및 서명 검증을 제공합니다. 이미지 서명은 이미지를 저장하기 전에 확인됩니다. **Image** 서비스에 업로드하려면 기존 이미지에 암호화 서명을 추가해야 합니다. 이 서명은 부팅 시 이미지를 검증하는 데 사용됩니다. **OpenStack Key Manager**는 서명 키에 대한 키 관리 지원을 제공합니다.

Object Storage - 미사용 데이터 암호화 및 OpenStack Key Manager 지원

Object Storage(swift) 서비스는 이제 **OpenStack Key Manager**(barbican)에 저장된 256비트 키로 **CTR** 모드에서 **AES**를 사용하여 암호화된 형식으로 개체를 저장할 수 있습니다. 한번 **Director**를 사용하여 암호화가 **Object Storage**에 활성화되면 시스템은 클러스터에서 모든 개체를 암호화하는 데 사용되는 단일 키를 생성합니다. 단일 키는 **Object Storage** 클러스터에서 개체를 보호하고 보안 컴플라이언스를 유지하기 위한 옵션을 제공합니다.

Shared File System - Shared File System 서비스의 컨테이너화된 배포

이번 릴리스에서 **Shared File System** 서비스(manila)의 컨테이너화된 배포는 기본 기능입니다. 이 서비스에 외부 설치 종속성을 지닌 백엔드를 사용하는 경우 배포에 대한 벤더별 컨테이너를 가져와야 합니다.

Shared File System - NetApp ONTAP cDOT 드라이버를 사용한 IPv6 액세스 규칙 지원

Shared File System 서비스(manila)는 이제 **IPv6** 네트워크에서 **NetApp ONTAP** 백엔드가 지원하는 내보내기 공유를 지원합니다. 내보내기된 공유에 대한 액세스는 **IPv6** 클라이언트 주소에 의해 제어됩니다.

2.13. 기술 프리뷰

이 섹션에서는 **Red Hat OpenStack Platform 13**의 기술 프리뷰에 소개된 기능에 대해 간단히 설명합니다.



참고

기술 프리뷰로 표시된 기능의 지원 범위에 대한 자세한 내용은 [기술 프리뷰 기능 지원 범위](#)를 참조하십시오.

2.13.1. 새로운 기술 프리뷰

다음과 같은 새로운 기능은 기술 프리뷰로 제공됩니다.

Ansible 기반 설정 (config download)

Director는 이제 오버클라우드 계획을 기본으로 사용하여 **Ansible Playbook** 세트를 생성할 수 있습니다. 이는 오버클라우드 설정 방식을 **OpenStack Orchestration(heat)**에서 **Ansible** 기반 방식으로 변경합니다. 업그레이드와 같이 지원되는 일부 **OpenStack Platform 13** 기능은 이 기능을 프로세서의 일부로 사용합니다. 그러나 지원되는 영역 외 사용은 프로덕션 환경에서는 권장되지 않으며 기술 프리뷰로만 사용할 수 있습니다.

OVS 하드웨어 오프로드

OVS(Open vSwitch) 하드웨어 오프로드는 과도한 작업을 SmartNIC가 포함된 하드웨어로 이동하여 OVS를 가속합니다. 이는 OVS 처리를 SmartNIC에 오프로드하여 호스트 리소스가 절약됩니다.

2.13.2. 이전에 릴리스된 기술 프리뷰

다음 기능은 기술 프리뷰로 계속 제공됩니다.

Benchmarking 서비스

Rally는 다중 노드 OpenStack 배포, 클라우드 검증, 벤치마킹 및 프로파일링을 자동화하고 통합하는 벤치마킹 도구로서 SLA, 성능 및 안정성을 지속적으로 향상할 수 있는 OpenStack CI/CD 시스템의 기본 도구로 사용할 수 있습니다. 다음과 같은 핵심 구성 요소로 구성됩니다.

- 서버 공급자 - 다양한 가상화 기술(LXS, Virsh 등) 및 클라우드 공급업체와의 상호 작용을 위한 통합 인터페이스를 제공합니다. ssh 액세스와 하나의 L3 네트워크를 통해 통합 인터페이스를 제공합니다.
- 배포 엔진 - 서버 공급자에서 검색한 서버를 사용하여 벤치마킹 절차 시작 전에 OpenStack을 배포합니다.
- 검증 - 배포된 클라우드에 대한 특정 테스트 세트를 실행하여 올바르게 작동하는지 확인하고 결과를 수집하여 해당 결과를 사람이 읽을 수 있는 형식으로 제공합니다.
- 벤치마크 엔진 - 매개 변수화된 벤치마크 시나리오를 작성하고 클라우드에서 수행합니다.

Benchmarking 서비스 - 새로운 플러그인 유형, 후크 도입

테스트 시나리오를 반복 실행할 수 있으며 실행된 작업에 대한 타임스탬프(및 기타 정보)를 Rally 보고서에 제공할 수 있습니다.

Benchmarking 서비스 - 새로운 시나리오

nova, cinder, magnum, ceilometer, manila 및 neutron에 대한 Benchmarking 시나리오가 추가되었습니다.

Benchmarking 서비스 - 검증 구성 요소의 리팩토링

Rally Verify는 Tempest를 시작하는 데 사용됩니다. 검사기 유형, 검사기 및 검사 결과와 같은 새로운 모델을 포함하도록 리팩토링되었습니다.

셀

OpenStack Compute는 컴퓨팅 리소스를 분할하기 위해 **nova-cells** 패키지에서 제공하는 셀 개념을 포함합니다. 이 릴리스에서는 **Cells v1**이 **Cells v2**로 대체되었습니다. Red Hat OpenStack Platform은 기본 구성으로 "단일 셀"을 배포하지만 현재는 다중 셀 배포를 지원하지 않습니다.

DNSaaS(DNS-as-a-Service)

Designate로 알려진 DNSaaS(DNS-as-a-Service)에는 도메인 및 레코드 관리를 위한 REST API가 구현되어 있으며 멀티 테넌트를 지원하고 인증을 위해 OpenStack Identity 서비스(keystone)와 통합됩니다. DNSaaS에는 Compute(nova) 및 OpenStack Networking(neutron) 알림과의 통합을 위한 프레임워크가 포함되어 있어 DNS 레코드의 자동 생성이 가능합니다. DNSaaS에는 Bind9 백엔드와의 통합이 구현되어 있습니다.

FWaaS(Firewall-as-a-Service)

FWaaS(Firewall-as-a-Service) 플러그인은 OpenStack Networking(neutron)에 경계 방화벽 관리 기능을 제공합니다. FWaaS는 iptables를 사용하여 프로젝트 내의 모든 가상 라우터에 방화벽 정책을 적용하고 프로젝트마다 1개의 방화벽 정책과 논리 방화벽 인스턴스를 지원합니다. FWaaS는 네트워크 경계에서 작동하며 OpenStack Networking(neutron) 라우터에서 트래픽을 필터링합니다. 이는 인스턴스 수준에서 작동하는 보안 그룹과 다릅니다.

Google 클라우드 스토리지 백업 드라이버(Block Storage)

이제 Google 클라우드 스토리지를 사용하여 볼륨 백업을 저장하도록 Block Storage(cinder) 서비스를 구성할 수 있습니다. 이 기능을 사용하면 큰 비용이 드는 재해 복구 전용 백업 클라우드를 유지 관리할 필요가 없습니다.

베어 메탈 노드용 링크 집계

이번 릴리스에서는 베어 메탈 노드에 대한 링크 집계가 도입되었습니다. 링크 집계를 사용하면 페일오버 및 로드 밸런싱을 지원하도록 베어 메탈 노드 NIC에서 본딩을 구성할 수 있습니다. 이 기능을 사용하려면 전용 neutron 플러그인에서 구성할 수 있는 특정 하드웨어 스위치 벤더 지원이 필요합니다. 하드웨어 벤더 스위치가 올바른 neutron 플러그인을 지원하는지 확인하십시오.

또는 베어 메탈 노드에 본딩을 설정하도록 스위치를 수동으로 사전 구성할 수 있습니다. 노드가 본딩 인터페이스 중 하나를 부팅할 수 있게 하려면 스위치가 LACP 및 LACP 폴백을 지원해야 합니다 (본딩이 형성되지 않은 경우 본딩 링크는 개별 링크로 폴백됨). 그렇지 않은 경우 노드는 별도의 프로비저닝 및 정리 네트워크가 필요합니다.

Red Hat OpenStack Platform for POWER

이제 IBM POWER8 little endian 하드웨어에서 사전 프로비저닝된 오버클라우드 Compute 노드를 배포할 수 있습니다.

Red Hat SSO

이번 릴리스에는 keycloak-httpd-client-install 패키지 버전이 포함되어 있습니다. 이 패키지는 Apache mod_auth_mellon SAML 서비스 공급자를 Keycloak SAML IdP의 클라이언트로 구성하는 데 도움이 되는 명령행 도구를 제공합니다.

3장. 릴리스 정보

본 릴리스 노트에서는 Red Hat OpenStack Platform 릴리스를 배포할 때 고려해야 할 기술 프리뷰 항목, 권장 사항, 알려진 문제 및 사용되지 않는 기능에 대해 설명합니다.

Red Hat OpenStack Platform 릴리스의 지원 라이프사이클 중에 출시된 업데이트에 대한 정보는 각 업데이트와 관련된 권고 설명에 표시됩니다.

3.1. RED HAT OPENSTACK PLATFORM 13 GA

본 릴리스 노트에서는 Red Hat OpenStack Platform 릴리스를 배포할 때 고려해야 할 기술 프리뷰 항목, 권장 사항, 알려진 문제 및 사용되지 않는 기능에 대해 설명합니다.

3.1.1. 기능 개선

이번 Red Hat OpenStack Platform 릴리스에는 다음과 같은 개선된 기능이 포함되어 있습니다.

BZ#1419556

Object Store 서비스(swift)는 이제 Barbican과 통합하여 저장된(미사용) 개체를 투명하게 암호화하고 해독할 수 있습니다. 미사용 암호화는 전송중인 암호화와는 다르며 디스크에 저장되는 동안 암호화되는 개체를 참조합니다.

Swift 개체는 디스크에서 일반 텍스트로 저장됩니다. 이러한 디스크는 라이프 사이클 종료에 도달했을 때 적절히 폐기되지 않으면 보안 위험을 발생시킬 수 있습니다. 개체 암호화는 이러한 위험을 완화합니다.

Swift는 swift에 업로드 시 자동으로 암호화되고 사용자에게 제공 시 자동으로 해독되는 개체를 사용하여 암호화 작업을 투명하게 수행합니다. 이 암호화 및 해독은 Barbican에 저장되는 동일한 (symmetric) 키를 사용하여 처리됩니다.

BZ#1540239

이 개선 사항은 매트릭스 데이터를 Gnocchi DB 인스턴스에 보내는 기능을 추가 지원합니다.

collectd 구성 가능한 서비스에 대해 다음의 새 매개 변수가 추가되었습니다. CollectdGnocchiAuthMode가 'simple'로 설정되면 CollectdGnocchiProtocol, CollectdGnocchiServer, CollectdGnocchiPort 및 CollectdGnocchiUser가 설정에 고려됩니다.

CollectdGnocchiAuthMode가 'keystone'으로 설정되면 CollectdGnocchiKeystone* 매개 변수가 설정에 고려됩니다.

추가된 매개 변수에 대한 자세한 설명은 다음과 같습니다.

CollectdGnocchiAuthMode:

유형: 문자열

설명: >

Gnocchi 서버가 사용하는 인증 유형입니다. 지원되는 값은 'simple' 및 'keystone'입니다.

기본값: 'simple'

CollectdGnocchiProtocol:

유형: 문자열

설명: Gnocchi 서버가 사용하는 API 프로토콜입니다.

```

기본값: 'http'
CollectdGnocchiServer:
  유형: 문자열
  설명: >
    매트릭스를 보내야 하는 gnocchi 엔드포인트의 이름 또는 주소입니다.
  기본값: nil
CollectdGnocchiPort:
  유형: 숫자
  설명: Gnocchi 서버에서 연결할 포트입니다.
  기본값: 8041
CollectdGnocchiUser:
  유형: 문자열
  설명: >
    simple 인증을 사용하여 원격 Gnocchi 서버에 인증을 위한 사용자 이름입니다.
  기본값: nil
CollectdGnocchiKeystoneAuthUrl:
  유형: 문자열
  설명: 인증할 Keystone 엔드포인트 URL입니다.
  기본값: nil
CollectdGnocchiKeystoneUserName:
  유형: 문자열
  설명: Keystone에 대해 인증을 위한 사용자 이름입니다.
  기본값: nil
CollectdGnocchiKeystoneUserId:
  유형: 문자열
  설명: Keystone에 대해 인증을 위한 사용자 ID입니다.
  기본값: nil
CollectdGnocchiKeystonePassword:
  유형: 문자열
  설명: Keystone에 대해 인증을 위한 암호입니다.
  기본값: nil
CollectdGnocchiKeystoneProjectId:
  유형: 문자열
  설명: Keystone에 대해 인증을 위한 프로젝트 ID입니다.
  기본값: nil
CollectdGnocchiKeystoneProjectName:
  유형: 문자열
  설명: Keystone에 대해 인증을 위한 프로젝트 이름입니다.
  기본값: nil
CollectdGnocchiKeystoneUserDomainId:
  유형: 문자열
  설명: Keystone에 대해 인증을 위한 사용자 도메인 ID입니다.
  기본값: nil
CollectdGnocchiKeystoneUserDomainName:
  유형: 문자열
  설명: Keystone에 대해 인증을 위한 사용자 도메인 이름입니다.
  기본값: nil
CollectdGnocchiKeystoneProjectDomainId:
  유형: 문자열
  설명: Keystone에 대해 인증을 위한 프로젝트 도메인 ID입니다.
  기본값: nil
CollectdGnocchiKeystoneProjectDomainName:
  유형: 문자열
  설명: Keystone에 대해 인증을 위한 프로젝트 도메인 이름입니다.
  기본값: nil
CollectdGnocchiKeystoneRegionName:

```

```

    유형: 문자열
    설명: Keystone에 대해 인증을 위한 지역 이름입니다.
    기본값: nil
CollectdGnocchiKeystoneInterface:
    유형: 문자열
    설명: 인증할 Keystone 엔드포인트의 유형입니다.
    기본값: nil
CollectdGnocchiKeystoneEndpoint:
    유형: 문자열
    설명: >
        Keystone 값을 덮어쓰기하려는 경우 명백하게 Gnocchi 서버 URL을 지정합니다.
    기본값: nil
CollectdGnocchiResourceType:
    유형: 문자열
    설명: >
        호스트를 저장하기 위해 Gnocchi에서 collectd-gnocchi 플러그인으로 생성된 기본 리
소스 유형입니다.
    기본값: 'collectd'
CollectdGnocchiBatchSize:
    유형: 숫자
    설명: Gnocchi에서 일괄 처리해야 하는 값의 최소 개수입니다.
    기본값: 10

```

3.1.2. 기술 프리뷰

이 섹션에 나열된 항목은 기술 프리뷰로 제공됩니다. 기술 프리뷰 상태 범위에 대한 자세한 내용 및 관련된 지원 영향은 <https://access.redhat.com/support/offerings/techpreview/>에서 참조하십시오.

BZ#1488095

RHOS-12 이상에서 OpenStack 서비스는 컨테이너화되어 있습니다. 이번 릴리스에서는 OpenStack Tempest도 컨테이너화되었습니다. 컨테이너화된 OpenStack Tempest는 기술 프리뷰로 사용할 수 있습니다.

3.1.3. 릴리스 노트

본 섹션에서는 Red Hat OpenStack Platform에 대한 권장 사항 및 중요한 변경 사항을 포함하여 이번 릴리스 관련 중요한 세부 사항을 간단히 설명합니다. 배포에 대해 가능한 최상의 결과를 얻으려면 이 정보를 반드시 숙지하셔야 합니다.

BZ#1468020

Shared File System 서비스(manila)는 이제 NetApp ONTAP cDOT 드라이버가 포함된 IPv6 액세스 규칙을 지원하여 IPv6 환경으로 manila를 사용할 수 있습니다.

따라서 Shared File System 서비스는 이제 IPv6 네트워크에서 NetApp ONTAP 백엔드가 지원하는 내보내기 공유를 지원합니다. 내보내기의 공유에 대한 액세스는 IPv6 클라이언트 주소에서 이루어집니다.

BZ#1469208

Shared File System 서비스(manila)는 NFSv4 프로토콜을 통해 CephFS(Ceph File System)에서 지원하는 공유 파일 시스템 마운트를 지원합니다. 컨트롤러 노드에서 실행되는 NFS-Ganesha 서버는 CephFS를 고가용성(HA)의 테넌트로 내보내는 데 사용됩니다. 테넌트는 서로 격

리되며 제공된 NFS 게이트웨이 인터페이스를 통해서만 CephFS에 액세스할 수 있습니다. 이 새로운 기능은 director에 모두 통합되어 CephFS 백엔드 배포 및 Shared File System 서비스의 설정을 가능하게 합니다.

BZ#1496584

Neutron 서비스가 컨테이너화되면 네트워크 네임스페이스에서의 명령 실행 시도는 다음 오류와 함께 실패할 수 있습니다.

```
# ip netns exec qrouter...
RTNETLINK answers: Invalid argument
```

네트워크 네임스페이스 내부에서 명령을 실행하려면 해당 네임스페이스를 생성한 neutron 컨테이너에서 명령을 수행해야 합니다. 예를 들어 l3-agent는 라우터에 대한 네트워크 네임스페이스를 생성하므로 명령을 다음과 같이 변경합니다.

```
# docker exec neutron_l3_agent ip netns exec qrouter...
```

'qdhcp'로 시작하는 네트워크 네임스페이스와 유사하게 'neutron_dhcp' 컨테이너에서 명령을 실행해야 합니다.

BZ#1503521

이 버전은 networking-ovn에서 내부 DNS 변환을 지원합니다. 두 개의 알려진 제한이 있으며 하나는 내부 DNS를 통해 내부 FQDN 요청이 제대로 해결되지 않는 bz#1581332입니다.

GA 릴리스에서 tripleo는 기본적으로 이러한 확장 기능이 설정되지 않습니다. bz#1577592에서 해결 방법을 참조하십시오.

BZ#1533206

openstack-gnocchi 패키지 이름이 gnocchi로 변경되었습니다. openstack- 접두사는 업스트림 프로젝트 범위 변경으로 인해 삭제되었습니다. Gnocchi는 OpenStack의 산하에서 벗어나 독립형 프로젝트로 유지됩니다.

BZ#1556933

버전 2.1부터 python-cryptography는 인증서에 사용된 CNS 이름이 IDN 표준에 부합하는지 확인합니다. 검색된 이름이 이 사양을 따르지 않는 경우 cryptography는 인증서를 검증할 수 없게 되며 OpenStack 명령줄 인터페이스를 사용하는 경우 또는 OpenStack 서비스 로그에서 다른 오류가 발견될 수 있습니다.

BZ#1563412

OpenStack Compute(nova) 용으로 예약된 호스트 메모리가 2048MB에서 4096MB로 증가했습니다. 이는 환경의 용량 추정에 영향을 줄 수 있습니다. 필요한 경우 환경 파일에서 'NovaReservedHostMemory' 매개 변수를 사용하여 예약된 메모리를 다시 설정할 수 있습니다. 예를 들면 다음과 같습니다.

```
parameter_defaults:
    NovaReservedHostMemory: 2048
```

BZ#1564176

`python-mistralclient`는 지원되는 오버클라우드 사용 사례에 포함되어 있지 않으므로 OSP 13 릴리스의 `-tools` 채널에서 삭제되었습니다.

BZ#1567735

OVN을 네트워킹 백엔드로 사용하는 OSP13의 첫 번째 릴리스에는 IPv6 지원이 포함되지 않습니다. 따라서 게스트 VM의 Neighbor Solicitation 요청에 대한 응답에 문제가 있어 기본 경로가 손실됩니다.

BZ#1575752

이전 버전에서 `*NetName` 매개 변수(예: `InternalApiNetName`)는 기본 네트워크의 이름을 변경했습니다. 이는 현재 더 이상 지원되지 않습니다.

기본 네트워크의 이름을 변경하려면 구성 가능한 사용자 지정 네트워크 파일 (`network_data.yaml`)을 사용하여 `'openstack overcloud deploy'` 명령에 `'-n'` 옵션을 포함합니다. 이 파일에서 `"name_lower"` 필드를 변경하려는 네트워크의 사용자 지정 네트워크 이름으로 설정해야 합니다. 자세한 내용은 오버클라우드 고급 사용자 지정 가이드에서 "구성 가능한 네트워크 사용"을 참조하십시오.

또한 `ServiceNetMap` 테이블에 대한 로컬 매개 변수를 `network_environment.yaml`에 추가하고 이전 네트워크 이름에 대한 모든 기본값을 새 사용자 지정 이름으로 덮어쓰기 해야 합니다. 기본값은 `/usr/share/openstack-tripleo-heat-templates/network/service_net_map.j2.yaml`에서 확인할 수 있습니다. 향후 OSP-13 릴리스에서는 `ServiceNetMap`을 수정할 필요가 없습니다.

BZ#1577537

OSP 13 베타에서 일부 컨테이너 이미지를 사용할 수 없는 문제가 수정되었습니다.

BZ#1578312

OVSDB 서버가 다른 컨트롤러 노드에서 오류가 발생하면 이 상태가 감지되지 않기 때문에 `neutron-server/metadata-agent`에서 다시 연결되지 않습니다.

그 결과 VM 부팅은 `metadata-agent`로 작동할 수 없으며 새 메타데이터 네임스페이스를 프로비저닝하지 않고 클러스터링이 예상대로 동작하지 않습니다.

이 문제는 새 컨트롤러가 OVN 데이터베이스에 대한 마스터로 승격된 후 모든 Compute 노드에서 `ovn_metadata_agent` 컨테이너를 다시 시작하여 해결할 수 있습니다. 또한 `plugin.ini`에서 `ovsdb_probe_interval`을 600000밀리초의 값으로 증가하여 해결할 수 있습니다.

BZ#1589849

OVN 메타데이터 에이전트가 Compute 노드에서 중지되면 해당 노드에 있는 모든 VM가 메타데이터 서비스에 액세스할 수 없습니다. 그 영향으로 새 VM이 생성되거나 기존 VM이 재부팅되는 경우 OVN 메타데이터 에이전트를 다시 가져올 때까지 VM이 메타데이터에 액세스할 수 없게 됩니다.

BZ#1592528

극히 드물게 컨트롤러 노드를 여러 번 재부팅한 후 RabbitMQ의 상태가 일정하지 않게되어 오버클라우드의 API 작업이 차단될 수 있습니다.

이 문제의 증상은 다음과 같습니다.

- OpenStack 서비스 로그에 다음과 같은 항목이 표시됩니다:
DuplicateMessageError: Found duplicate message(629ff0024219488499b0fac0cacao3a5). Skipping it.
- "openstack network agent list"는 일부 에이전트가 정지(DOWN)상태로 반환됩니다.

일반 작업을 복구하려면 컨트롤러 노드에서 다음 명령을 실행합니다(하나의 컨트롤러에서만 이를 수행해야 함).

```
pcs resource restart rabbitmq-bundle
```

3.1.4. 알려진 문제

현재 Red Hat OpenStack Platform에 있는 알려진 문제는 다음과 같습니다.

BZ#1321179

`python-requests`를 사용하는 OpenStack 명령행 클라이언트는 현재 SAN 필드에 IP 주소가 있는 인증서를 확인할 수 없습니다.

BZ#1461132

Cinder 볼륨 및 Cinder 백업에 대한 Block Storage 백엔드로 Red Hat Ceph Storage를 사용하는 경우 증분 백업을 시도하면 아무런 경고 없이 전체 백업이 대신 수행됩니다. 이는 알려진 문제입니다.

BZ#1508449

OVN은 compute 노드에서 직접 ovn-controller를 사용하는 DHCP를 openflow 컨트롤러로 사용합니다. 하지만 SR-IOV 인스턴스는 VF/PF를 통해 네트워크에 직접 연결됩니다. 이와 같이 SR-IOV 인스턴스는 어디에서도 DHCP 응답을 얻을 수 없게 됩니다.

이 문제를 해결하려면 OS::TripleO::Services::NeutronDhcpAgent를 다음으로 변경합니다.

```
OS::TripleO::Services::NeutronDhcpAgent: docker/services/neutron-dhcp.yaml
```

BZ#1515815

라우터 게이트웨이가 지워지면 식별된 IP 주소와 관련된 Layer 3 흐름이 삭제되지 않습니다. 식별된 IP 주소에는 PNF 및 외부 게이트웨이 IP 주소가 포함됩니다. 이로 인해 흐름이 오래되지만, 기능적 문제는 발생하지 않습니다. 외부 게이트웨이 및 IP 주소는 자주 변경되지 않습니다. 오래된 흐름은 외부 네트워크가 삭제될 때 삭제됩니다.

BZ#1518126

Redis는 TLS를 활성화된 HA 배포 노드에서 데이터를 올바르게 복제할 수 없습니다. Redis 팔로워 노드는 리더 노드의 데이터를 포함하지 않습니다. Redis 배포에 대해 TLS를 비활성화하는 것이 좋습니다.

BZ#1519783

Neutron은 Quota가 Neutron 라우터 생성에 대해 초과하였음을 나타내는 오류가 표시될 수 있습니다. 이는 알려진 문제로서 networking-odl이 포함된 버그로 인해 다중 라우터 리소스가

Neutron DB의 단일 생성 요청으로 생성되는 문제입니다. 이 문제는 OpenStack Neutron CLI를 사용하여 중복된 라우터를 삭제하고 라우터를 다시 생성하여 단일 인스턴스의 결과를 가져와 해결할 수 있습니다.

BZ#1557794

회귀가 director 언더클라우드의 백업 및 복구 절차에서 식별되었습니다. 그 결과, 프로세스를 수정 및 검증해야 릴리즈할 수 있습니다.

따라서 문서 'Director 언더클라우드 백업 및 복구'는 Red Hat OpenStack Platform 13의 일반 릴리스 버전에서 제공되지 않습니다. 프로세스는 일반 릴리스 이후 우선순위로 업데이트되며 확인되는 즉시 게시됩니다.

BZ#1559055

OpenDaylight 로깅에서 이전 로그가 누락될 수 있습니다. 이는 OpenDaylight의 journald 로깅으로 알려진 문제입니다("docker logs opendaylight_api" 명령 사용). 현재 컨테이너의 내부에서 /opt/opendaylight/data/logs/karaf.log에 로그할 "file" 메커니즘으로 OpenDaylight 로깅을 전환하여 해결할 수 있습니다. 문제 해결을 위해 다음 heat 매개 변수를 설정합니다. OpenDaylightLogMechanism: 'file'.

BZ#1562035

Docker는 nsenter 호출에 대한 커널 오류로 인해 docker-puppet 또는 paunch 컨테이너를 실행하는 동안 실행에 실패합니다. 이는 fork 함수의 unshare 호출 사용과 관련된 커널 문제로 식별되었습니다. 수정 사항은 RHEL 7.5.2 릴리스와 관련된 다음 커널 릴리스에서 제공됩니다(6월 말로 예정). BZ #1577745와 관련된 커널 핫픽스는 요청에 따라 제공될 수 있습니다.

또는 다음 해결 방법을 사용할 수 있습니다.

1) 환경 파일에서 "TunedProfileName" 매개 변수를 삭제하고 배포합니다. cpu-partitioning없이 배포하는 경우 재현성이 더 낮은 것으로 확인되고 있습니다. 배포가 완료되면 다음 단계로 tuned 프로파일을 활성화합니다.

- * "isolated_cores" in /etc/tuned/cpu-partitioning-variables.conf 설정
- * "tuned-adm profile cpu-partitioning" 명령 실행
- * 노드 다시 시작

참고: 이 해결 방법을 사용하면 문제가 발생할 가능성이 낮은 것으로 확인되고 있습니다.

2) 코멘트에 지정된 명령을 따릅니다. https://bugzilla.redhat.com/show_bug.cgi?id=1562035#c27 및 https://bugzilla.redhat.com/show_bug.cgi?id=1562035#c31

참고: 원하는 결과가 아닌 호스트 PID를 컨테이너에 노출하면 컨테이너가 실행됩니다. 자세한 단계는 OSP13의 다음 마이너 릴리스에 제공되므로 이 문제를 해결하기 위해 "pid=host" 방법이 더 이상 필요하지 않습니다.

BZ#1568012

유동 IP를 인스턴스에 연결한 다음 유동 IP 연결을 해제하는 경우 외부 IP에 대한 연결에 오류가 발생합니다. 이 상황은 VM이 비 NAPT Switch에 생성된 경우 유동 IP가 삭제된 유동 IP와 연결 시 테넌트 VLAN 네트워크에서 발생합니다. 이를 통해 NAPT Switch의 FIB 테이블에서 누락된 흐름이 (산발적으로) 발생합니다.

누락된 FIB 테이블 항목 때문에 VM에서는 공용 네트워크에 대한 연결이 손실됩니다.

유동 IP를 VM에 연결하면 공용 네트워크에 대한 연결을 복원합니다. 유동 IP가 VM에 연결되어 있는 한 인터넷에 연결할 수 있습니다. 그러나 외부 네트워크에서 공용 IP/유동 IP가 손실됩니다.

■
BZ#1568311

유동 IP가 할당되지 않은 인스턴스가 다른 라우터에서 유동 IP가 할당된 다른 인스턴스에 연결 시도하는 경우 다중 서브넷의 Nova 인스턴스 간 Layer 3 연결이 실패할 수 있습니다. 이는 Nova 인스턴스가 다중 compute 노드에 분산되는 경우 발생합니다. 현재 이 문제에 적합한 해결 방법은 없습니다.

BZ#1568976

하나 이상의 OpenDaylight 인스턴스는 배포 또는 기능적 오류로 이어질 수 있는 기능 로딩 버그 때문에 배포 동안 올바르게 시작하지 못할 수 있습니다.

이 상황에서는 다음 작업을 실행하십시오.

- * HA 배포에서 두 개 이상의 OpenDaylight 인스턴스가 올바른 부팅에 필요하며 그렇지 않으면 배포가 실패할 수 있습니다. 이 경우 현재 'docker ps' 명령을 사용하여 각 컨테이너의 상태를 확인하는 방법으로 문제를 해결할 수 있습니다. 상태가 비정상이라면 컨테이너를 다시 시작합니다 ('docker restart opendaylight_api').

- * TLS 기반의 배포에서 모든 OpenDaylight 인스턴스를 올바르게 부팅하지 않으면 배포에 실패합니다. 이로 인해 모든 OpenDaylights가 성공적으로 부팅될 때까지 배포를 다시 시작해야 합니다.

BZ#1571864

빠른 업그레이드 준비 동안 Heat 스택 리소스의 임시 삭제는 RHEL 등록 취소를 트리거합니다. 그 결과 Heat 소프트웨어 배포 시그널링이 적절하게 작동하지 않으므로 RHEL 등록 취소가 정지됩니다.

이 문제를 해결하려면 오버클라우드가 아직 OSP 10에 있는 동안 최신 오버클라우드 마이너 버전 업데이트를 수행할 준비를 하십시오.

1. 템플릿 파일 /usr/share/openstack-tripleo-heat-templates/extraconfig/pre_deploy/rhel-registration/rhel-registration.yaml을 편집합니다.
2. 템플릿에서 RHELUnregistration 및 RHELUnregistrationDeployment 리소스를 삭제합니다.
3. 마이너 업데이트 및 빠른 업그레이드 절차를 진행합니다.

BZ#1573597

Gnocchi 백엔드로 성능이 낮은 Swift 클러스터가 사용되면 collectd 로그에서 503 오류를 생성하고 gnocchi-metricd.conf에서 "ConnectionError: ('Connection aborted.', CannotSendRequest())" 오류를 출력할 수 있습니다.

이 문제를 해결하려면 CollectdDefaultPollingInterval 매개 변수의 값을 증가시키거나 Swift 클러스터 성능을 개선합니다.

BZ#1574708

OpenDaylight 인스턴스가 클러스터에서 삭제되고 다시 연결되면 인스턴스가 클러스터에 성공적으로 참여할 수 없는 경우가 있습니다. 노드는 결과적으로 클러스터에 다시 참여하게 됩니다.

이러한 상황에서 다음 작업을 수행해야 합니다.

- * 문제가 있는 노드를 다시 시작합니다.
- * REST 엔드포인트를 모니터링하여 클러스터 구성원이 정상인지 상태를 확인합니다.

`http://$ODL_IP:8081/jolokia/read/org.opendaylight.controller:Category=ShardManager,name=shard-manager-config,type=DistributedConfigDatastore`
 * 응답에는 "SyncStatus" 필드가 포함되어야 하며 값이 "true"인 경우 클러스터 구성원이 정상적임을 나타냅니다.

BZ#1574725

VLAN 공급자의 동일한 서브넷에서 다중 VM이 두 개의 다른 Compute 노드에 스케줄링되면 VM 간 ARP가 실패하는 경우가 있습니다.

이러한 VM 간 ARP 패킷 전송이 실패하므로 두 개의 VM 간에는 실질적으로 네트워킹이 없는 것입니다.

BZ#1575023

ceph-ansible의 복잡한 ceph-key 작업을 변경하면 `/etc/ceph/ceph.client.manila.keyring` 파일에서 잘못된 콘텐츠를 생성하므로 manila-share 서비스가 초기화에 실패합니다.

manila-share 서비스 초기화를 허용하려면 다음을 수행합니다.

1) 오버클라우드 배포에 사용할 `/usr/share/openstack/tripleo-heat-templates`의 사본을 만듭니다.

2) 295행에서 모든 삼중 백슬래시를 단일 백슬래시로 변경하도록 `.../tripleo-heat-templates/docker/services/ceph-ansible/ceph-base.yaml` 파일을 편집합니다.

편집 전:

```
mon_cap: 'allow r, allow command \\\\"auth del\\\\" , allow command \\\\"auth caps\\\\" , allow command \\\\"auth get\\\\" , allow command \\\\"auth get-or-create\\\\"'
```

편집 후:

```
mon_cap: 'allow r, allow command \"auth del\" , allow command \"auth caps\" , allow command \"auth get\" , allow command \"auth get-or-create\"'
```

3) `/usr/share/openstack-tripleo-heat` 템플릿이 기존 `overcloud-deploy` 명령에서 발생하는 위치마다 `tripleo-heat-templates`의 사본에 대한 경로를 대체하는 오버클라우드를 배포합니다.

ceph 키 `/etc/ceph/ceph.client.manila.keyring` 파일에는 알맞은 콘텐츠가 있으며 manila-share 서비스는 적절히 초기화됩니다.

BZ#1575118

Ceph 릴리스 12.2.1은 각 OSD에 허용된 최대 PG 개수를 낮춥니다. 한도를 낮추면 모니터가 HEALTH_WARN 메시지를 조기에 제기할 수 있습니다.

모니터 경고 임계값은 OSD당 300PG에서 200PG로 줄어들었습니다. 200은 OSD당 100PG의 일반 권장 대상의 두 배입니다. 이 한도는 모니터에서 `mon_max_pg_per_osd` 옵션을 통해 조정할 수 있습니다. 이전 `mon_pg_warn_max_per_osd` 옵션은 삭제되었습니다.

풀에서 사용하는 PG의 양은 줄일 수 없습니다. 업그레이드로 인해 기존에 존재하는 배포가 최대한 도에 도달하면 ceph-upgrade 단계 동안 한도를 사전 업그레이드 값으로 올릴 수 있습니다. 환경 파일에서 다음과 같은 매개 변수 설정을 추가하십시오.

```
parameter_defaults:
  CephConfigOverrides:
```

```
mon_max_pg_per_osd: 300
```

이 설정은 `ceph.conf`에 적용되며 클러스터는 `HEALTH_OK` 상태로 유지됩니다.

BZ#1575150

OpenDaylight 클러스터 구성원이 (오류 등의 이유로 인해) 중지된 경우 최대 30분 간 OpenDaylight 클러스터가 응답하지 않는 알려진 문제가 있습니다. 이 문제를 해결하려면 클러스터가 다시 활성화될 때까지 기다려야 합니다.

BZ#1575496

Director로 외부 네트워크에 대한 물리적 호스트 인터페이스를 사용하는 경우 인터페이스가 OVS 브릿지에 연결되지 않으면 인터페이스가 OpenDaylight 설정에서 트래픽을 통과하지 않으므로 이러한 설정을 피해야 합니다.

오버클라우드 외부 네트워크 용 NIC 템플릿에서 OVS 브릿지를 항상 사용합니다. 이 브릿지는 어떤 이름도 사용할 수 있지만 Director에서 기본적으로 "br-ex"입니다. 외부 네트워크에 사용되는 물리적 호스트 인터페이스를 OVS 브릿지에 연결해야 합니다.

OVS 브릿지에 연결된 인터페이스를 사용하는 경우 배포는 올바르게 기능하며 테넌트에 대한 외부 네트워크 트래픽이 올바르게 작동합니다.

BZ#1577975

OpenDaylight는 일정 기간 동안 CPU 사용량이 매우 높아질 수 있습니다. 이 문제는 잠재적으로 다른 시스템 서비스에 영향을 줄 수 있지만 OpenDaylight의 기능에 영향을 미치지 않습니다.

BZ#1579025

OVN Pacemaker RA(Resource Agent) 스크립트에서는 Pacemaker가 슬레이브 노드 승격을 시도할 때 프로모션 작업을 적절하게 처리하지 않는 경우가 있습니다. 이는 마스터 IP가 노드로 이동할 때 `ovsdb-servers`가 RA 스크립트의 상태를 마스터로 보고하여 발생합니다. 해당 문제는 업스트림에서 수정되었습니다.

문제가 발생하면 neutron 서버가 OVN North 및 South DB 서버에 연결할 수 없게 되며 neutron 서버에 대한 모든 Create/Update/Delete API에 오류가 발생합니다.

`ovn-dbs-bundle` 리소스를 다시 시작하면 문제가 해결됩니다. 컨트롤러 노드 중 하나에서 아래 명령을 실행하십시오.

```
"pcs resource restart ovn-dbs-bundle"
```

BZ#1579417

SNAT 지원에는 테넌트 네트워크에서 사용되는 캡슐화와 상관없이 VXLAN 터널 설정이 필요합니다. 또한 VXLAN 터널 헤더가 페이로드에 추가되어 패킷이 기본 MTU(1500바이트)를 초과할 수 있으므로 VLAN 테넌트 네트워크를 사용하는 경우 MTU를 올바르게 설정해야 합니다.

VXLAN 터널은 SNAT 트래픽을 통과시키기 위해서 올바르게 구성해야 합니다.

VLAN 테넌트 네트워크를 사용하는 경우 SNAT 트래픽이 VXLAN 터널을 통해 흐를 수 있도록 다음 방식 중 하나를 사용하여 MTU를 설정합니다.

- * VLAN 테넌트 기반 네트워크를 설정하여 네트워크 설정당 1450의 MTU를 사용합니다.
- * `NeutronGlobalPhysnetMtu` heat 매개 변수를 1450으로 설정합니다. 참고: 이는 모든

flat/VLAN공급자 네트워크가 1450MTU가 되는 것을 의미하므로 바람직하지 않을 수 있습니다.
(특히 외부 공급자 네트워크의 경우)

* 1550(또는 이상)의 MTU로 테넌트 네트워크 언더레이를 설정합니다. 여기에는 테넌트 네트워크 NIC에 대해 NIC 템플릿에서 MTU를 설정하는 작업이 포함됩니다.

BZ#1581337

PING 유형 상태 모니터를 사용하려면 HAProxy(드라이버에서 네트워크 로드 밸런싱에 사용하는 기본 소프트웨어) 버전은 1.6 이상이어야 합니다. 이전 HAProxy 버전을 사용하면 사용자 확인 없이 TCP 연결 상태가 확인됩니다.

업스트림 커뮤니티에서는 코드에 확인을 추가하여 사용 중인 HAProxy 버전을 확인하고 그에 따라 작동하도록 수정했습니다.

HAProxy 버전이 1.6 이상이면 PING를 사용할 수 있습니다.

그렇지 않은 경우 TCP 연결을 계속 사용합니다(이러한 HAProxy 버전에 대한 다른 솔루션이 없으면 이 방법이 효과적입니다).

OSP13 GA의 문제는 이전 버전의 HAProxy를 사용하는 RHEL 채널 일부로 HAProxy를 탑재하는 것입니다. 따라서 OSP13 사용자가 PING 유형 상태 모니터를 설정하는 경우 TCP 연결을 대신 가져옵니다.

BZ#1583541

SRIOV 기반 Compute 인스턴스는 서로 다른 네트워크에 있는 경우 OVS Compute 인스턴스에 연결되지 않습니다. VLAN 공급자 네트워크 모두에 연결된 외부 라우터를 사용하여 이 문제를 해결할 수 있습니다.

BZ#1584518

RHOSP는 nova에서 기본적으로 DifferentHostFilter/SameHostFilter의 가용성을 설정하지 않으며 해당 설정은 일부 테스트를 완료하는 데 필요합니다. 따라서 일부 보안 그룹 테스트는 무작위로 실패할 수 있습니다.

이러한 테스트를 건너뛰거나 이러한 필터를 nova 설정에 추가해야 합니다.

BZ#1584762

Telemetry가 언더클라우드에서 수동으로 활성화되면 `hardware.*` 매트릭스는 각 노드에 있는 잘못된 방화벽 설정으로 인해 작동하지 않습니다.

이를 해결하기 위해 다음과 같이 언더클라우드 배포에 여분의 템플릿을 추가하여 컨트롤 플레인 네트워크에서 `snmpd` 서브넷을 수동으로 설정해야 합니다.

```
parameter_defaults:
  SnmpdIpSubnet: 192.168.24.0/24
```

BZ#1588186

경합 조건으로 인해 Open vSwitch는 Opendaylight openflowplugin에 연결되지 않습니다. 이 제품의 13.z 릴리스에서 이 문제를 해결할 예정입니다.

BZ#1590114

Telemetry가 언더클라우드에서 수동으로 활성화되면 `hardware.*` 매트릭스는 각 노드에 있는

잘못된 방화벽 설정으로 인해 작동하지 않습니다.

이를 해결하기 위해 다음과 같이 언더클라우드 배포에 여분의 템플릿을 추가하여 컨트롤 플레인 네트워크에서 `snmpd` 서버넷을 수동으로 설정해야 합니다.

```
parameter_defaults:
  SnmpdIpSubnet: 192.168.24.0/24
```

BZ#1590560

ceph-anatitle 유틸리티는 ceph-create-keys 컨테이너가 생성된 동일한 노드에서 이를 항상 삭제하지는 않습니다.

이 때문에 배포는 "Error response from daemon: No such container: ceph-create-keys." 메시지와 함께 실패할 수 있습니다. 이로 인해 하나 이상의 compute 노드가 있는 새로운 배포나 ceph 클라이언트로 작동하는 사용자 지정 역할을 포함하여 Ceph를 사용하는 서비스를 호스팅하는 ceph-ansible 실행에 영향을 미칠 수 있습니다.

BZ#1590938

RHCS3에서 세 개 이상의 OSD를 배포하고 pgcalc(<https://access.redhat.com/labs/cephpgc>)에서 결정한 대로 풀에 PG 개수를 설정하면 모든 OSD가 활성화되기 전에 ceph-ansible이 풀을 생성하므로 배포에 실패합니다.

이 문제를 해결하려면 기본 PG 개수를 32로 설정하고 배포가 완료되면 Storage Strategies Guide (https://access.redhat.com/documentation/en-us/red_hat_ceph_storage/3/html/storage_strategies_guide/placement_groups_pg#set_the_number_of_pgs)에 설명된 대로 PG 개수를 수동으로 올립니다.

BZ#1590939

ceph-ansible OpenStack 풀 작업에 잘못된 컨테이너 이름이 있으므로 아직 Ceph MON 및 OSD를 같이 배치할 수 없습니다.

표준 HCI(Compute + OSD)는 영향을 받지 않습니다.

BZ#1593290

SR-IOV 기반 네트워크 인터페이스가 연결된 게스트가 실행 중인 상태에서 nova-compute 서비스를 다시 시작한 후 게스트를 삭제하면 해당 노드에서 SR-IOV VF를 게스트에 더 이상 연결할 수 없습니다. 이는 서비스 시작 시 사용 가능한 장치가 열거되지만 장치가 게스트에 연결되므로 호스트 장치 목록에 포함되지 않기 때문입니다.

게스트를 삭제하고 나면 'nova-compute' 서비스를 다시 시작해야 합니다. 게스트를 삭제하고 서비스를 다시 시작한 후에 사용 가능한 SR-IOV 장치 목록이 올바르게 나열됩니다.

BZ#1593715

비보안 레지스트리 목록은 주요 업그레이드 동안 일부 컨테이너 이미지를 가져온 이후에 업데이트되기 때문에 새로 도입된 비보안 레지스트리의 컨테이너 이미지는 `openstack overcloud upgrade run` 명령 동안 다운로드할 수 없습니다.

다음 해결 방법을 사용할 수 있습니다.

옵션 A: Pacemaker에서 관리하는 컨테이너가 있는 노드에서 수동으로

/etc/sysconfig/docker 파일을 업데이트하고 새로 도입된 비보안 레지스트리를 추가합니다.

옵션 B: 업그레이드 직전에 `openstack overcloud deploy` 명령을 실행하고 DockerInsecureRegistryAddress 매개 변수가 포함된 환경 파일을 사용하여 원하는 새로운 비보안 레지스트리 목록을 제공합니다.

모든 컨테이너 이미지는 업그레이드 동안 성공적으로 다운로드해야 합니다.

BZ#1593757

기존 오버클라우드 배포에서 Octavia를 활성화하면 성공으로 보고하지만 컨트롤러 노드에서 방화벽 규칙이 잘못 설정되어 Octavia API 엔드포인트에는 연결할 수 없습니다.

해결 방법:

모든 컨트롤러 노드에서 방화벽 규칙을 추가하고 DROP 규칙 전에 삽입되었는지 확인합니다.

IPv4:

```
# iptables -A INPUT -p tcp -m multiport --dports 9876 -m state --state NEW -m comment --comment "100 octavia_api_haproxy ipv4" -j ACCEPT
# iptables -A INPUT -p tcp -m multiport --dports 13876 -m state --state NEW -m comment --comment "100 octavia_api_haproxy_ssl ipv4" -j ACCEPT
# iptables -A INPUT -p tcp -m multiport --dports 9876,13876 -m state --state NEW -m comment --comment "120 octavia_api ipv4" -j ACCEPT
```

IPv6:

```
# ip6tables -A INPUT -p tcp -m multiport --dports 9876 -m state --state NEW -m comment --comment "100 octavia_api_haproxy ipv6" -j ACCEPT
# ip6tables -A INPUT -p tcp -m multiport --dports 13876 -m state --state NEW -m comment --comment "100 octavia_api_haproxy_ssl ipv6" -j ACCEPT
# ip6tables -A INPUT -p tcp -m multiport --dports 9876,13876 -m state --state NEW -m comment --comment "120 octavia_api ipv6" -j ACCEPT
```

HAProxy를 다시 시작합니다:

```
# docker restart haproxy-bundle-docker-0
```

BZ#1595363

빠른 업그레이드 프로세스 동안 사용자는 언더클라우드를 버전 10에서 버전 11로 업그레이드합니다. 일부 상황에서는 nova-api.log가 다음 오류를 보고할 수 있습니다.

```
`Unexpected API Error. Table 'nova_cell10.instances' doesn't exist`
```

다음 명령을 실행하여 이 오류를 해결할 수 있습니다.

```
$ sudo nova-manage api_db sync
```

이 문제는 중요하지 않으며 빠른 업그레이드 프로세스에 큰 영향을 주지 않아야 합니다.

4장. 기술 노트

이 장에서는 콘텐츠 전송 네트워크를 통해 제공되는 Red Hat OpenStack Platform "Queens" 에라타 권고의 추가 정보를 제공합니다.

4.1. RHEA-2018:2086 – RED HAT OPENSTACK PLATFORM 13.0 강화 권고

이 섹션에 포함된 버그는 RHEA-2018:2086 권고에 의해 해결되었습니다. 이 권고에 대한 자세한 내용은 <https://access.redhat.com/errata/RHEA-2018:2086> 링크에서 확인하십시오.

ceph-ansible

BZ#1590560

ceph-ansible 유틸리티는 ceph-create-keys 컨테이너를 생성된 동일한 노드에서 항상 삭제하지 않습니다.

따라서 "Error response from daemon: No such container: ceph-create-keys." 메시지가 표시되고 배포에 실패할 수 있습니다. 이로 인해 다음의 새로운 배포가 포함된 ceph-ansible 실행에 영향을 줄 수 있습니다.

- * 다중 compute 노드 또는
- * ceph를 사용하는 서비스를 호스팅하는 ceph 클라이언트로 동작하는 사용자 지정 역할

gnocchi

BZ#1533206

openstack-gnocchi 패키지 이름이 gnocchi로 변경되었습니다. openstack- 접두사는 업스트림 프로젝트 범위 변경으로 인해 삭제되었습니다. Gnocchi는 OpenStack의 산하에서 벗어나 독립형 프로젝트로 유지됩니다.

opendaylight

BZ#1568012

유동 IP를 인스턴스에 연결한 다음 유동 IP 연결을 해제하는 경우 외부 IP에 대한 연결에 오류가 발생합니다. 이 상황은 다음의 경우 테넌트 VLAN 네트워크에서 발생합니다.

- * 비 NAPT 스위치에서 생성된 VM이 유동 IP와 연결된 경우
- * 유동 IP가 삭제된 경우

이를 통해 NAPT 스위치의 FIB 테이블에서 누락된 흐름이 (산발적으로) 발생합니다.

누락된 FIB 테이블 항목 때문에 VM에서는 공용 네트워크에 대한 연결이 손실됩니다.

유동 IP를 VM에 연결하면 공용 네트워크에 대한 연결을 복원합니다. 유동 IP가 VM에 연결되는 있는 한 인터넷에 연결할 수 있지만 외부 네트워크의 공용 IP/유동 IP가 손실됩니다.

openstack-cinder

BZ#1557331

이전에는 롤링 업그레이드 메커니즘 때문에 오프라인으로 업그레이드할 때 cinder 서비스를 두 번

다시 시작해야 했습니다.

"--bump-versions"라는 새로운 선택 매개 변수를 `cinder-manage db sync` 명령에 추가하여 두 시스템 재부팅을 건너뛸 수 있습니다.

BZ#1572220

Block Storage Service(cinder)는 동기화 잠금을 사용하여 볼륨 이미지 캐시의 항목이 중복 되는 것을 방지합니다. 하지만 이러한 유형의 잠금은 범위가 광범위하므로 이미지 캐시가 활성화되지 않은 경우에도 이미지에서 볼륨 생성 요청이 동시에 발생하면 잠금 작업을 위해 경쟁할 수 있습니다.

이미지에서 볼륨을 생성하는 동시 요청은 연속적으로 실행되며 동시에 실행되지 않습니다.

이를 해결하기 위해 동기화 잠금은 잠금 범위를 최소화하고 볼륨 이미지 캐시가 활성화된 경우에만 적용되도록 업데이트되었습니다.

이번 릴리스에서는 이미지에서 볼륨 생성 동시 요청은 볼륨 이미지 캐시가 비활성화된 경우 동시에 실행됩니다. 볼륨 이미지 캐시가 활성화되면 단일 항목만 캐시에서 생성되도록 잠금을 최소화할 수 있습니다.

openstack-manila

BZ#1468020

Shared File System 서비스(manila)는 이제 NetApp ONTAP cDOT 드라이버가 포함된 IPv6 액세스 규칙을 지원하여 IPv6 환경으로 manila를 사용할 수 있습니다.

따라서 Shared File System 서비스는 이제 IPv6 네트워크에서 NetApp ONTAP 백엔드가 지원하는 내보내기 공유를 지원합니다. 내보내기된 공유에 대한 액세스는 IPv6 클라이언트 주소에서 제어됩니다.

BZ#1469208

Shared File System 서비스(manila)는 NFSv4 프로토콜을 통해 CephFS(Ceph File System)에서 지원하는 공유 파일 시스템 마운트를 지원합니다. 컨트롤러 노드에서 실행되는 NFS-Ganesha 서버는 CephFS를 고가용성(HA)의 테넌트로 내보내는 데 사용됩니다. 테넌트는 서로 격리되며 제공된 NFS 게이트웨이 인터페이스를 통해서만 CephFS에 액세스할 수 있습니다. 이 새로운 기능은 director에 모두 통합되어 CephFS 백엔드 배포 및 Shared File System 서비스의 설정을 가능하게 합니다.

openstack-neutron

BZ#1552108

라우터에서 인터페이스를 추가하거나 삭제할 때 격리된 메타데이터가 DHCP 에이전트에서 활성화되는 경우 해당 네트워크에 대한 메타데이터 프록시는 업데이트되지 않습니다.

이와 같이 인스턴스가 라우터에 연결되지 않은 네트워크에 있다면 메타데이터를 가져올 수 없습니다.

라우터 인터페이스가 추가되거나 삭제되면 메타데이터 프록시를 업데이트해야 합니다. 그러면 인스턴스는 사용하는 네트워크가 격리된 경우 DHCP 네임스페이스에서 메타데이터를 가져올 수 있게 됩니다.

openstack-selinux

BZ#1561711

이전 릴리스에서는 게스트 가상 머신이 시작되면 virtlogd 서비스가 중복 AVC 거부 오류를 기록했습니다. 이번 업데이트를 통해 virtlogd 서비스는 더 이상 systemd에 종료 비활성화 호출을 전송하지 않으므로 위의 오류가 더 이상 발생하지 않습니다.

openstack-swift

BZ#1419556

Object Store 서비스(swift)는 이제 Barbican과 통합하여 저장된(미사용) 개체를 투명하게 암호화하고 해독할 수 있습니다. 미사용 암호화는 전송중인 암호화와는 다르며 디스크에 저장되는 동안 암호화되는 개체를 참조합니다.

Swift 개체는 디스크에서 일반 텍스트로 저장됩니다. 이러한 디스크는 라이프 사이클 종료에 도달했을 때 적절히 폐기되지 않으면 보안 위험을 발생시킬 수 있습니다. 개체 암호화는 이러한 위험을 완화합니다.

Swift는 swift에 업로드 시 자동으로 암호화되고 사용자에게 제공 시 자동으로 해독되는 개체를 사용하여 암호화 작업을 투명하게 수행합니다. 이 암호화 및 해독은 Barbican에 저장되는 동일한 (symmetric) 키를 사용하여 처리됩니다.

openstack-tripleo-common

BZ#1560422

Octavia는 "service" 프로젝트에 설정된 기본 쿼터가 오버클라우드에서 생성될 수 있는 Octavia 로드 밸런서의 개수를 제한하므로 실제 워크로드로 확장되지 않습니다.

이 문제를 해결하려면 오버클라우드 admin 사용자로서 필요한 쿼터를 무제한 또는 충분히 큰 값으로 설정합니다. 예를 들어 언더클라우드에서 다음 명령을 실행합니다.

```
# source ~/overcloudrc
# openstack quota set --cores -1 --ram -1 --ports -1 --instances -1 --
  secgroups -1 service
```

BZ#1588838

tripleo.plan_management.v1.update_roles 워크플로는 오버클라우드 계획 이름(swift 컨테이너 이름) 또는 zaqar 대기열 이름을 트리거된 하위 워크플로에 전달할 수 없습니다. 이로 인해 기본값('overcloud')이 아닌 오버클라우드 계획 이름을 사용하면 잘못된 동작이 발생했습니다. 이번 수정을 통해 이러한 매개 변수를 올바르게 전달하고 올바른 동작을 복구합니다.

BZ#1566463

'docker kill' 명령은 컨테이너가 자동으로 다시 시작하도록 설정된 경우 종료되지 않습니다. 사용자가 'docker kill <container>'를 시도하면 무기한으로 중단될 수 있습니다. 이 경우

CTRL+C로 명령을 중지합니다.

이 문제를 해결하려면 'docker stop'('docker kill' 대신)을 사용하여 컨테이너화된 서비스를 중지합니다.

BZ#1452979

원인: "openstack overcloud node configure" 명령은 "deploy-kernel" 및 "deploy-ramdisk" 매개 변수에 대해 이미지 ID가 아닌 이미지 이름만 가져옵니다. 이번 수정 후 이미지 ID가 허용됩니다.

openstack-tripleo-heat-templates

BZ#1341176

이번 기능 개선으로 "regular" compute 노드를 통해 director에서 compute 노드가 활성화된 RT 배포를 추가 지원합니다.

1. tripleo-heat-templates/environments/compute-real-time-example.yaml을 기반으로 compute-real-time.yaml 환경 파일을 생성합니다. 이 파일은 ComputeRealTime 역할의 매개 변수 중 최소한 다음 매개 변수를 올바른 값으로 설정합니다.

* IsolCpusList 및 NovaVcpuPinSet: 실시간 워크로드에 대해 예약되어야 하는 CPU 코어의 목록입니다. 이는 실시간 compute 노드에 있는 CPU 하드웨어에 따라 달라집니다.

* KernelArgs: "default_hugepagesz=1G hugepagesz=1G hugepages=X"로 설정합니다. X는 게스트 수 및 예약할 메모리 양에 따라 달라집니다.

2. overcloud-realtime-compute 이미지를 빌드하고 업로드합니다.

* 리포지토리 준비(CentOS용):

```
- sudo yum install -y
```

```
https://trunk.rdoproject.org/centos7/current/python2-tripleo-repos-XXX.el7.centos.noarch.rpm
```

```
- sudo -E tripleo-repos current-tripleo-dev
```

```
- export DIB_YUM_REPO_CONF="/etc/yum.repos.d/delorean*  
/etc/yum.repos.d/quickstart"
```

```
* openstack overcloud image build --image-name overcloud-realtime-compute  
--config-file /usr/share/openstack-tripleo-common/image-yaml/overcloud-  
realtime-compute.yaml --config-file /usr/share/openstack-tripleo-  
common/image-yaml/overcloud-realtime-compute-centos7.yaml
```

```
* openstack overcloud image upload --update-existing --os-image-name  
overcloud-realtime-compute.qcow2
```

3. ComputeRealTime 및 다른 모든 필수 역할로 roles_data.yaml을 생성하고(예: openstack overcloud roles generate -o ~/rt_roles_data.yaml Controller ComputeRealTime ...) ComputeRealTime 역할을 일반적인 방법의 하나로 실시간 노드에 할당합니다. https://docs.openstack.org/tripleo-docs/latest/install/advanced_deployment/custom_roles.html을 참조하십시오.

4. 오버클라우드를 배포합니다.

```
openstack overcloud deploy --templates -r ~/rt_roles_data.yaml -e
./tripleo-heat-templates/environments/host-config-and-reboot.yaml -e
./compute-real-time.yaml [...]
```

BZ#1552583

HA 설정에서 glance-direct 방식을 사용 시 공유 준비 영역이 필요합니다. 일반 준비 영역이 없으면 HA 환경에서 'glance-direct' 방식을 사용한 이미지 업로드가 실패할 수 있습니다. 컨트롤러 노드에서 수신하는 요청은 사용 가능한 컨트롤러 노드에 배포됩니다. 하나의 컨트롤러가 첫 번째 단계를 처리하며 다른 컨트롤러는 이미지를 다른 준비 영역에 작성하는 컨트롤러를 모두 사용하여 두 번째 요청을 처리합니다. 두 번째 컨트롤러에는 첫 번째 단계를 처리하는 컨트롤러가 사용하는 동일한 준비 영역에 대한 액세스 권한이 없습니다.

Glance는 'glance-direct' 방식을 포함한 다중 이미지 가져오기 방식을 지원합니다. 이 방식은 3단계 방식을 사용합니다(이미지 레코드 생성, 준비 영역에 이미지 업로드, 이미지를 사용할 수 있도록 준비 영역에서 스토리지 백엔드로 이미지 전송). HA 설정에서(예: 3개의 컨트롤러 노드 사용) glance-direct 방식은 컨트롤러 노드 전반에 공유 파일 시스템을 사용하는 일반 준비 영역이 필요합니다.

활성화된 Glance 가져오기 방식 목록을 이제 설정할 수 있습니다. 기본 설정은 'glance-direct' 방식을 활성화하지 않습니다 (웹 다운로드를 기본적으로 활성화됨). 이 문제를 해결하여 HA 환경에서 이미지를 Glance에 안정적으로 가져오려면 'glance-direct' 방식을 활성화하지 마십시오.

BZ#1572238

openvswitch systemd 스크립트는 호스트에서 정지 시 /run/openvswitch 폴더를 삭제합니다.

ovn-controller 컨테이너 내 /run/openvswitch 경로는 이전 디렉토리입니다. 서비스를 다시 시작하는 경우 폴더를 다시 생성합니다. ovn-controller에서 이 폴더로 다시 액세스하려면 폴더를 다시 마운트하거나 ovn-controller 컨테이너를 다시 시작해야 합니다.

BZ#1309550

Cinder 용 RBD 백엔드로 사용하는 Ceph 풀 목록을 지정하는 새로운 CinderRbdExtraPools Heat 매개 변수가 추가되었습니다. 추가 Cinder RBD 백엔드 드라이버는 목록에서 각 풀에 대해 생성됩니다. 이는 CinderRbdPoolName과 연결된 표준 RBD 백엔드 드라이버에 추가됩니다. 새로운 매개 변수는 선택 사항이며 기본적으로 빈 목록입니다. 모든 풀은 단일 Ceph 클러스터와 연결됩니다.

BZ#1518126

Redis는 TLS를 활성화된 HA 배포 노드에서 데이터를 올바르게 복제할 수 없습니다. Redis 팔로워 노드는 리더 노드의 데이터를 포함하지 않습니다. Redis 배포에 대해 TLS를 비활성화하는 것이 좋습니다.

BZ#1540239

이번 개선 사항으로 매트릭스 데이터를 Gnocchi DB 인스턴스에 보내는 기능을 추가 지원합니다.

collectd 구성 가능한 서비스에 대해 다음의 새 매개 변수가 추가되었습니다. CollectdGnocchiAuthMode가 'simple'로 설정되면 CollectdGnocchiProtocol,

CollectdGnocchiServer, CollectdGnocchiPort 및 CollectdGnocchiUser가 설정에 고려됩니다.

CollectdGnocchiAuthMode가 'keystone'으로 설정되면 CollectdGnocchiKeystone* 매개 변수가 설정에 고려됩니다.

다음은 추가된 매개 변수에 대한 자세한 설명입니다.

CollectdGnocchiAuthMode:

유형: 문자열

설명: >

Gnocchi 서버가 사용하는 인증 유형입니다. 지원되는 값은 'simple' 및 'keystone'입니다.

기본값: 'simple'

CollectdGnocchiProtocol:

유형: 문자열

설명: Gnocchi 서버가 사용하는 API 프로토콜입니다.

기본값: 'http'

CollectdGnocchiServer:

유형: 문자열

설명: >

매트릭스를 보내야 하는 gnocchi 엔드포인트의 이름 또는 주소입니다.

기본값: nil

CollectdGnocchiPort:

유형: 숫자

설명: Gnocchi 서버에서 연결할 포트입니다.

기본값: 8041

CollectdGnocchiUser:

유형: 문자열

설명: >

simple 인증을 사용하여 원격 Gnocchi 서버에 인증을 위한 사용자 이름입니다.

기본값: nil

CollectdGnocchiKeystoneAuthUrl:

유형: 문자열

설명: 인증할 Keystone 엔드포인트 URL입니다.

기본값: nil

CollectdGnocchiKeystoneUserName:

유형: 문자열

설명: Keystone에 대해 인증을 위한 사용자 이름입니다.

기본값: nil

CollectdGnocchiKeystoneUserId:

유형: 문자열

설명: Keystone에 대해 인증을 위한 사용자 ID입니다.

기본값: nil

CollectdGnocchiKeystonePassword:

유형: 문자열

설명: Keystone에 대해 인증을 위한 암호입니다.

기본값: nil

CollectdGnocchiKeystoneProjectId:

유형: 문자열

설명: Keystone에 대해 인증을 위한 프로젝트 ID입니다.

기본값: nil

CollectdGnocchiKeystoneProjectName:

유형: 문자열

설명: Keystone에 대해 인증을 위한 프로젝트 이름입니다.

기본값: nil

CollectdGnocchiKeystoneUserId:

유형: 문자열

설명: Keystone에 대해 인증을 위한 사용자 도메인 ID입니다.

기본값: nil

CollectdGnocchiKeystoneUserName:

유형: 문자열

설명: Keystone에 대해 인증을 위한 사용자 도메인 이름입니다.

기본값: nil

CollectdGnocchiKeystoneProjectDomainId:

유형: 문자열

설명: Keystone에 대해 인증을 위한 프로젝트 도메인 ID입니다.

기본값: nil

CollectdGnocchiKeystoneProjectDomainName:

유형: 문자열

설명: Keystone에 대해 인증을 위한 프로젝트 도메인 이름입니다.

기본값: nil

CollectdGnocchiKeystoneRegionName:

유형: 문자열

설명: Keystone에 대해 인증을 위한 지역 이름입니다.

기본값: nil

CollectdGnocchiKeystoneInterface:

유형: 문자열

설명: 인증할 Keystone 엔드포인트의 유형입니다.

기본값: nil

CollectdGnocchiKeystoneEndpoint:

유형: 문자열

설명: >

Keystone 값을 덮어쓰기하려는 경우 명백하게 Gnocchi 서버 URL을 지정합니다.

기본값: nil

CollectdGnocchiResourceType:

유형: 문자열

설명: >

호스트를 저장하기 위해 Gnocchi에서 collectd-gnocchi 플러그인으로 생성된 기본 리소스 유형입니다.

기본값: 'collectd'

CollectdGnocchiBatchSize:

유형: 숫자

설명: Gnocchi에서 일괄 처리해야 하는 값의 최소 개수입니다.

기본값: 10

BZ#1566376

OVN 메타데이터 서비스는 DVR 기반 환경에 배포되지 않았습니다. 따라서 인스턴스는 인스턴스 이름, 공개 키 등의 메타데이터를 가져올 수 없었습니다.

이 패치는 부팅된 인스턴스가 메타데이터를 가져오도록 위의 서비스를 활성화합니다.

BZ#1568120

Cinder 백엔드 서비스의 Heat 템플릿은 서비스가 컨테이너에 배포되어야 하는지 여부와 상관없이 Puppet을 트리거하고 오버클라우드 호스트에 cinder-volume 서비스를 배포하도록 했습니다. 이로 인해 cinder-volume 서비스가 컨테이너와 호스트에 두 번 배포되었습니다.

이 때문에 호스트에서 실행 중인 독자적인 cinder-volume 서비스에서 작업을 처리한 경우 OpenStack 볼륨 작업(볼륨 생성 및 연결)이 일반적으로 실패할 수도 있었습니다.

문제 해결을 위해 Cinder 백엔드 heat 템플릿은 cinder-volume 서비스의 두 번째 인스턴스를 배포하지 않도록 업데이트되었습니다.

BZ#1573597

Gnocchi 백엔드로 성능이 낮은 Swift 클러스터가 사용되면 collectd 로그에서 503 오류를 생성하고 gnocchi-metricd.conf에서 "ConnectionError: ('Connection aborted.', CannotSendRequest())" 오류를 출력할 수 있습니다.

이 문제를 해결하려면 CollectdDefaultPollingInterval 매개 변수의 값을 증가시키거나 Swift 클러스터 성능을 개선합니다.

BZ#1575023

ceph-ansible의 복잡한 ceph-key 작업을 변경하면 /etc/ceph/ceph.client.manila.keyring 파일에서 잘못된 콘텐츠를 생성하므로 manila-share 서비스가 초기화에 실패합니다.

manila-share 서비스 초기화를 허용하려면 다음을 수행합니다.

1) 오버클라우드 배포에 사용할 /usr/share/openstack/tripleo-heat-templates의 사본을 만듭니다.

2) 295행에서 모든 삼중 백슬래시를 단일 백슬래시로 변경하도록 .../tripleo-heat-templates/docker/services/ceph-ansible/ceph-base.yaml 파일을 편집합니다.

편집 전:

```
mon_cap: 'allow r, allow command \\\\"auth del\\\\" , allow command \\\\"auth caps\\\\" , allow command \\\\"auth get\\\\" , allow command \\\\"auth get-or-create\\\\"'
```

편집 후:

```
mon_cap: 'allow r, allow command \"auth del\" , allow command \"auth caps\" , allow command \"auth get\" , allow command \"auth get-or-create\"'
```

3) /usr/share/openstack-tripleo-heat 템플릿이 기존 overcloud-deploy 명령에서 발생하는 위치마다 tripleo-heat-templates의 사본에 대한 경로를 대체하는 오버클라우드를 배포합니다.

ceph 키 /etc/ceph/ceph.client.manila.keyring 파일에는 알맞은 콘텐츠가 있으며 manila-share 서비스는 적절히 초기화됩니다.

BZ#1552214

HA 용으로 cinder-volume 서비스를 구성할 때 cinder의 DEFAULT/host 설정이 "hostgroup"으로 설정되었습니다. 다른 cinder 서비스 (cinder-api, cinder-scheduler, cinder-backup)는 서비스를 실행하는 오버클라우드 노드와 상관없이 설정에 "hostgroup"을 사용했습니다. 이러한 서비스의 로그 메시지는 모두 동일한 "hostgroup" 호스트에서 시작된 것 같이 표시되어 메시지를 생성한 노드를 판단하기가 어려웠습니다.

HA를 배포할 때 cinder-volume의 backend_host는 DEFAULT/host를 해당 값으로 설정하는 대신 "hostgroup"으로 설정합니다. 이렇게 하면 각 노드의 DEFAULT/host 값이 고유한지 확인할 수 있습니다.

결과적으로 cinder-api, cinder-scheduler 및 cinder-backup의 로그 메시지는 메시지를 생성한 노드와 올바르게 연결됩니다.

BZ#1578901

새 릴리스로 업그레이드한 후 Block Storage Service(cinder)는 이전 릴리스에서 이전 RPC 버전을 사용하면 중단되었습니다. 이 때문에 최신 RPC 버전이 있어야 하는 모든 cinder API 요청은 실패했습니다.

새 릴리스로 업그레이드하는 경우 모든 cinder RPC 버전은 최신 릴리스와 일치하도록 업데이트됩니다.

python-cryptography**BZ#1556933**

버전 2.1부터 python-cryptography는 인증서에 사용된 CNS 이름이 IDN 표준에 부합하는지 확인합니다. 검색된 이름이 이 사양을 따르지 않는 경우 cryptography는 인증서를 검증할 수 없게 되며 OpenStack 명령줄 인터페이스를 사용하는 경우 또는 OpenStack 서비스 로그에서 다른 오류가 발견될 수 있습니다.

BZ#1571358

python-cryptography 빌드를 설치한 후 Obsoletes의 누락으로 인해 RDO에서 초기에 가져오기를 실행할 때 실패했습니다. 이 패키지의 RHEL 7 빌드는 적합한 Obsoletes 항목이 있습니다.

이번 수정에서 python-cryptography에 Obsoletes가 추가되었습니다.

python-ironic-tests-tempest**BZ#1577982**

업그레이드 전에 설치된 tempest 플러그인(-tests) rpm은 OSP Release 13 업그레이드 이후에 실패합니다. 초기 업그레이드 패키징에는 이전 rpm을 사용하지 않는 데 필요한 epoch 명령이 포함되지 않았습니다. sub-rpm은 OSP 13에 탑재되어 있지 않으며 새 플러그인 rpm의 Obsoletes는 적절한 rpm을 올바르게 폐기 처리하지 못했습니다.

이 문제를 해결하려면 Obsoletes를 수정하거나 이전 -rpm을 수동으로 설치 제거하고 교체 플러그인 python2-* -tests-tempest를 수동으로 설치합니다.

python-networking-ovn**BZ#1433533**

Neutron과 OVN 데이터베이스 간 일관성을 유지하기 위해 변경된 설정 내용이 내부에서 비교되며 백엔드에서 확인됩니다. 각 설정 변경에는 개정 번호가 할당되며 스케줄링된 작업은 데이터베이스에 추가된 모든 생성, 업데이트 및 삭제 작업을 확인합니다.

BZ#1503521

이 버전은 networking-ovn에서 내부 DNS 변환을 지원합니다. 두 개의 알려진 제한이 있으며 하나는 내부 DNS를 통해 내부 FQDN 요청이 제대로 해결되지 않는 bz#1581332입니다.

GA 릴리스에서 tripleo는 기본적으로 이러한 확장 기능이 설정되지 않습니다. bz#1577592에서 해결 방법을 참조하십시오.

BZ#1550039

게이트웨이 없이 서브넷이 생성되는 경우 DHCP 옵션이 추가되지 않으며 이러한 서브넷의 인스턴스는 DHCP를 가져올 수 없습니다.

인스턴스가 IP 주소를 가져오도록 Metadata/DHCP 포트가 이 작업에 사용됩니다. 메타데이터 서비스를 활성화해야 합니다. 서브넷의 인스턴스는 이제 외부 게이트웨이 없이 OVN Metadata/DHCP 포트를 통해 DHCP에서 IP 주소를 가져올 수 있습니다.

BZ#1562731

현재 L3 HA 스케줄러는 노드의 우선순위를 고려하고 있지 않습니다. 따라서 모든 게이트웨이는 동일한 노드에서 호스트되며 로드는 후보 노드에 배분되지 않았습니다.

이 수정은 게이트웨이 라우터를 스케줄링할 때 가장 적게 로드된 노드를 선택하도록 알고리즘을 구현합니다. 이제 시스템은 가장 적게 로드된 네트워크 노드에 스케줄링되어 게이트웨이 포트는 노드 간 로드를 균등하게 배분합니다.

BZ#1563678

하위 포트가 다른 하이퍼바이저의 다른 트렁크에 다시 할당된 경우 업데이트된 바인딩 정보를 가져오지 않으며 하위 포트가 ACTIVE로 전환되지 않았습니다.

이번 수정에서는 하위 포트가 트렁크에서 삭제되는 경우 바인딩 정보를 삭제합니다. 이제 하위 포트는 다른 하이퍼바이저에 있는 다른 트렁크에 다시 할당되는 경우 ACTIVE로 전환됩니다.

python-os-brick

BZ#1550974

iSCSI 검색을 사용하는 경우 노드 시작 설정이 "automatic"에서 "default"로 설정되어 재부팅 시 서비스가 시작되지 않았습니다. 이 문제는 각 검색 후 모든 시작 값을 복구하여 수정됩니다.

python-zaqar-tests-tempest

BZ#1546285

Queens 주기 동안 tempest 플러그인의 컬렉션이 openstack-*-tests rpm 하위 패키지에서 추출되었으므로 업그레이드에 종속성 문제가 있었습니다. 그러나 모든 패키징이 Provides 및 Obsoletes를 적합하게 결합한 것은 아닙니다. OSP 13에는 -tests(unittest sub-rpms)가 없습니다.

이전 릴리스에서 설치된 -tests로 업그레이드를 시도하는 경우 종속성 문제로 인해 업그레이드에 실패합니다.

이 문제를 해결하기 위해 추출되었던 -tests rpm의 이전 버전에 대한 Obsoletes가 다시 추가되었습니다.

